aws

Referência de autorização do serviço

Referência de autorização do serviço



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

Referência de autorização do serviço: Referência de autorização do serviço

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

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

Referência 1
Ações, recursos e chaves de condição 1
Tabela de ações 1
Tabela de tipos de recursos 2
Tabela de chaves de condição 3
AWS Gerenciamento de contas 18
AWS Ativar 25
Operações de IA da Amazon 28
Alexa for Business 40
AmazonMediaImport 59
AWS Amplificar 61
AWS Amplify Admin 71
AWS Amplify UI Builder 80
Apache Kafka para clusters APIs Amazon MSK 94
Amazon API Gateway 102
AWS App Mesh 105
AWS Pré-visualização do App Mesh 117
AWS Executor de aplicativos 125
AWS Estúdio de aplicativos 141
AWS Contêiner App2 145
AWS AppConfig 147
AWS AppFabric 163
Amazon AppFlow 173
Amazon AppIntegrations 182
AWS Application Auto Scaling 198
AWS Serviço Application Cost Profiler 206
Application Discovery Arsenal 209
AWS Application Discovery Service 212
AWS Serviço de migração de aplicativos 225
Amazon Application Recovery Controller – Mudança de zona 297
AWS Serviço de transformação de aplicativos 309
Amazon AppStream 2.0 313
AWS AppSync 338
Switch de região ARC da Amazon 356

AWS Artifato 362
Amazon Athena 367
AWS Audit Manager 383
Amazon Aurora DSQL 398
AWS Auto Scaling 405
AWS Intercâmbio de dados B2B 407
AWS Backup 415
AWS Gateway de backup 437
AWS Pesquisa de backup 444
AWS Armazenamento de backup 449
AWS Batch 453
Amazon Bedrock 472
Amazon Bedrock Agentcore 528
AWS Billing 548
AWS Billing e painéis de gerenciamento de custos 556
AWS Billing E exportações de dados de gerenciamento de custos 559
AWS Billing E calculadora de preços de gerenciamento de custos 564
AWS Billing E ações recomendadas pelo gerenciamento de custos 573
AWS Billing Conductor 575
AWS Billing Console 585
Amazon Braket 589
AWS Serviço de orçamento 594
AWS BugBust 600
AWS Certificate Manager 609
AWS Chatbot 616
Amazon Chime 627
AWS Salas limpas 697
AWS Salas limpas ML 733
Nuvem AWS API de controle 758
Amazon Cloud Directory 761
Nuvem AWS Mapa 775
AWS Cloud9 786
AWS CloudFormation 797
Amazon CloudFront 824
Amazon CloudFront KeyValueStore 853
AWS CloudHSM 856

Amazon CloudSearch 864
AWS CloudShell 871
AWS CloudTrail 875
AWS CloudTrail Dados 897
Amazon CloudWatch 900
Amazon CloudWatch Application Insights 915
Sinais CloudWatch de aplicativos da Amazon 921
Amazon, CloudWatch evidentemente 927
Monitor de CloudWatch Internet da Amazon 935
CloudWatch Registros da Amazon 940
Monitor sintético de CloudWatch rede Amazon 963
Gerenciador de acesso Amazon CloudWatch Observability 967
Serviço de administração CloudWatch do Amazon Observability 973
AWS CloudWatch RUM 980
Amazon CloudWatch Synthetics 986
AWS CodeArtifact 994
Amazon CodeCatalyst 1005
AWS CodeCommit 1016
AWS CodeConnections 1037
AWS CodeDeploy 1051
AWS CodeDeploy serviço de comandos de host seguro 1064
Amazon CodeGuru 1067
Amazon CodeGuru Profiler 1069
CodeGuru Revisor da Amazon 1075
CodeGuru Segurança da Amazon 1083
AWS CodePipeline 1088
AWS CodeStar 1099
AWS CodeStar Conexões 1106
AWS CodeStar Notificações 1122
Amazon CodeWhisperer 1131
Amazon Cognito Identity 1138
Amazon Cognito Sync 1146
Grupos de usuários do Amazon Cognito 1152
Amazon Comprehend 1172
Amazon Comprehend Medical 1209
AWS Otimizador de Computação 1215

AWS Config 1227
Amazon Connect Cases 1256
Amazon Connect Customer Profiles 1266
Campanhas externas do Amazon Connect 1284
Amazon Connect Voice ID 1292
AWS Serviço de conectores 1299
AWS Management Console Aplicativo móvel 1302
AWS Faturamento consolidado 1304
AWS Catálogo de controle 1306
AWS Control Tower 1310
AWS Relatório de custo e uso 1324
AWS Serviço Cost Explorer 1330
AWS Hub de otimização de custos 1345
AWS Serviço de verificação do cliente 1348
AWS Data Exchange 1351
Amazon Data Lifecycle Manager 1363
AWS Data Pipeline 1367
AWS Database Migration Service 1378
Database Query Metadata Service 1413
AWS DataSync 1417
Amazon DataZone 1432
AWS Nuvem de prazos 1460
AWS DeepComposer 1499
AWS DeepRacer 1506
Amazon Detective 1528
AWS Device Farm 1538
DevOps Guru da Amazon 1558
AWS Ferramentas de diagnóstico 1565
AWS Direct Connect 1570
AWS Directory Service 1587
AWS Dados do Directory Service 1617
Amazon DocumentDB Elastic Clusters 1628
Amazon DynamoDB 1650
Amazon DynamoDB Accelerator (DAX) 1675
Amazon EC2 Auto Scaling 1683
Amazon EC2 Image Builder 1712

Amazon EC2 Instance Connect 1748
Amazon EKS Auth 1753
AWS Elastic Beanstalk 1756
Amazon Elastic Block Store 1777
Amazon Elastic Container Registry 1782
Amazon Elastic Container Registry 1795
Amazon Elastic Container Service 1802
AWS Recuperação flexível de desastres 1835
Amazon Elastic File System 1871
Amazon Elastic Kubernetes Service 1883
AWS Elastic Load Balancing 1906
AWS Elastic Load Balancing V2 1923
Amazon Elastic MapReduce 1956
Amazon Elastic Transcoder 1976
Amazon Elastic VMware Service 1981
Amazon ElastiCache 1986
AWS Aparelhos e software elementares 2047
AWS Dispositivos elementares e serviço de ativação de software 2051
AWS Elemental MediaConnect 2055
AWS Elemental MediaConvert 2065
AWS Elemental MediaLive 2076
AWS Elemental MediaPackage 2104
AWS Elemental MediaPackage V2 2110
AWS VOD elementar MediaPackage 2122
AWS Elemental MediaStore 2129
AWS Elemental MediaTailor 2135
AWS Casos de suporte da Elemental 2147
AWS Conteúdo do Elemental Support 2153
Amazon EMR em EKS (EMR Containers) 2155
Amazon EMR Serverless 2164
AWS Mensagens SMS e voz para o usuário final V2 2170
AWS Mensagens sociais para usuários finais 2191
AWS Resolução de entidades 2198
Amazon EventBridge 2208
Amazon EventBridge Pipes 2227
Amazon EventBridge Scheduler 2232

EventBridge Esquemas da Amazon 2238
AWS Serviço de injeção de falhas 2246
Amazon FinSpace 2256
FinSpace API da Amazon 2271
AWS Gerenciador de Firewall 2273
Amazon Forecast 2285
Amazon Fraud Detector 2306
AWS Nível gratuito 2338
Amazon FreeRTOS 2341
Amazon FSx 2347
GameLift Servidores Amazon 2370
Amazon GameLift Streams 2399
AWS Acelerador global 2406
AWS Glue 2418
AWS Glue DataBrew 2476
AWS Ground Station 2487
GroundTruth Etiquetagem da Amazon 2496
Amazon GuardDuty 2501
AWS Health APIs e notificações 2520
AWS HealthImaging 2525
AWS HealthLake 2533
AWS HealthOmics 2540
Amazon Honeycode 2561
AWS Analisador de acesso IAM 2568
AWS Central de identidade do IAM 2576
AWS Diretório do IAM Identity Center 2604
AWS Serviço OIDC do IAM Identity Center 2615
AWS Identity and Access Management (IAM) 2618
AWS Funções de gerenciamento de identidade e acesso em qualquer lugar 2657
AWS Loja de identidades 2664
AWS Autenticação do Identity Store 2671
AWS Sincronizar identidade 2673
AWS Serviço de importação e exportação de disco 2678
Amazon Inspector 2681
Amazon Inspector2 2690
Amazon InspectorScan 2709

Amazon Interactive Video Service 2711
Chat do Amazon Interactive Video Service 2731
AWS Serviço de faturamento 2738
AWS IoT 1-Click 2743
AWS Análise de IoT 2750
AWS Consultor de dispositivos IoT Core 2758
AWS Testador de dispositivos IoT 2763
AWS Eventos de IoT 2766
AWS Hub de frota de IoT para gerenciamento de dispositivos 2775
AWS IoT FleetWise 2779
AWS Greengrass de IoT 2795
AWS IoT Greengrass V2 2817
AWS Empregos de IoT DataPlane 2829
AWS Integrações gerenciadas de IoT 2832
AWS IoT SiteWise 2849
AWS IoT TwinMaker 2870
AWS IoT Wireless 2882
AWS IQ 2907
AWS Permissões de QI 2917
Amazon Kendra 2921
Amazon Kendra Intelligent Ranking 2936
Amazon Keyspaces (for Apache Cassandra) 2940
Amazon Kinesis Analytics 2948
Amazon Kinesis Analytics V2 2953
Amazon Kinesis Data Streams 2960
Amazon Kinesis Firehose 2972
Amazon Kinesis Video Streams 2977
AWS Formação Lake Formation 2987
AWS Lambda 2998
AWS Launch Wizard 3017
Amazon Lex 3026
Amazon Lex V2 3036
AWS License Manager 3060
AWS License Manager Gerenciador de assinaturas Linux 3070
AWS Assinaturas de usuário do License Manager 3075
Amazon Lightsail 3083

Amazon Location 3121
Mapas do Amazon Location Service 3135
Locais do Amazon Location Service 3137
Rotas do Amazon Location Service 3141
Amazon Lookout for Equipment 3144
Amazon Lookout for Metrics 3156
Amazon Lookout for Vision 3164
Amazon Machine Learning 3171
Amazon Macie 3178
AWS Teste de aplicativos de modernização de mainframe 3198
AWS Serviço de modernização de mainframe 3207
Amazon Managed Blockchain 3218
Amazon Managed Blockchain Query 3229
Amazon Managed Grafana 3232
Amazon Managed Service for Prometheus 3240
Amazon Managed Streaming for Apache Kafka 3256
Amazon Managed Streaming for Kafka Connect 3274
Amazon Managed Workflows for Apache Airflow 3283
AWS Marketplace 3289
AWS Marketplace Catálogo 3296
AWS Marketplace Serviço de análise de comércio 3302
AWS Marketplace Serviço de implantação 3304
AWS Marketplace Descoberta 3309
AWS Marketplace Serviço de direitos 3311
AWS Marketplace Serviço de criação de imagens 3314
AWS Marketplace Portal de gerenciamento 3316
AWS Marketplace Serviço de medição 3321
AWS Marketplace Marketplace privado 3324
AWS Marketplace Integração de sistemas de compras 3328
AWS Marketplace Relatórios 3331
AWS Marketplace Relatórios do vendedor 3333
AWS Marketplace Insights do fornecedor 3336
Amazon Mechanical Turk 3344
Amazon MemoryDB 3353
Serviço de entrega de mensagens da Amazon 3377
Serviço Amazon Message Gateway 3380

AWS Extrator de microsserviços para.NET 3384
AWS Créditos do Migration Acceleration Program 3386
AWS Migration Hub 3389
AWS Orquestrador do Migration Hub 3398
AWS Refatorar espaços do Migration Hub 3406
AWS Recomendações da estratégia do Migration Hub 3427
Amazon Mobile Analytics 3434
Amazon Monitron 3436
Amazon MQ 3447
Aprovação de várias partes 3456
Amazon Neptune 3464
Amazon Neptune Analytics 3472
AWS Firewall de rede 3488
Monitor de fluxo de rede 3503
AWS Gerente de rede 3511
AWS Chat do gerente de rede 3536
Amazon Nimble Studio 3540
Amazon One Enterprise 3560
Amazon OpenSearch 3570
OpenSearch Ingestão da Amazon 3573
Amazon sem OpenSearch servidor 3580
OpenSearch Serviço Amazon 3589
AWS OpsWorks 3615
AWS OpsWorks Gerenciamento de configuração 3628
AWS Organizations 3633
AWS Outposts 3649
AWS Panorama 3657
AWS Serviço de computação paralela 3665
AWS Gerenciamento central de contas de parceiros 3678
AWS Central de vendas para parceiros 3681
AWS Criptografia de pagamento 3698
AWS Pagamentos 3708
AWS Insights de desempenho 3715
Amazon Personalize 3721
Amazon Pinpoint 3734
Serviço de e-mail do Amazon Pinpoint 3763

SMS e serviço de voz do Amazon Pinpoint 3779
Amazon Polly 3783
AWS Lista de preços 3786
AWS Conector CA privado para Active Directory 3789
AWS Conector CA privado para SCEP 3797
AWS Autoridade de certificação privada 3803
AWS PrivateLink 3810
AWS Proton 3812
AWS Console de pedidos de compra 3841
Amazon Q 3847
Amazon Q Business 3859
Aplicações do Amazon Q Business Q 3881
Amazon Q Developer 3898
Amazon Q in Connect 3902
Amazon QLDB 3925
Amazon QuickSight 3934
API Data do Amazon RDS 3982
Autenticação do IAM do Amazon RDS 3986
AWS Lixeira 3989
Amazon Redshift 3996
API de dados do Amazon Redshift 4042
Amazon Redshift sem servidor 4048
Amazon Rekognition 4067
AWS Repostagem privada 4084
AWS Centro de resiliência 4090
AWS Resource Access Manager (RAM) 4107
AWS Explorador de recursos 4126
API de marcação por etiquetas de resource groups da Amazon 4133
AWS Resource Groups 4137
Amazon RHEL Knowledgebase Portal 4145
AWS RoboMaker 4147
Amazon Route 53 4161
Domínios do Amazon Route 53 4179
Perfis do Amazon Route 53 4187
Amazon Route 53 Recovery Cluster 4194
Amazon Route 53 Recovery Controls 4197

Amazon Route 53 Recovery Readiness 4204
Amazon Route 53 Resolver 4213
Amazon S3 Express 4236
Amazon S3 Glacier 4273
Amazon S3 Object Lambda 4280
Amazon S3 on Outposts 4308
Tabelas do Amazon S3 4377
Vetores do Amazon S3 4386
Assistente SageMaker de ciência de dados da Amazon 4391
Capacidades SageMaker geoespaciais da Amazon 4394
Amazon SageMaker com MLflow 4402
AWS Savings Plans 4413
AWS Secrets Manager 4418
AWS Security Hub 4445
AWS Resposta a incidentes de segurança 4472
Amazon Security Lake 4478
AWS Serviço de migração de servidores 4510
AWS Serverless Application Repository 4517
AWS Serviço - Oracle Database@AWS 4522
AWS Service Catalog 4538
AWS Serviço para gerenciar recursos AWS Management Console de experiência do usuário. 4567
AWS serviço que fornece redes privadas gerenciadas 4569
Service Quotas 4577
Amazon SES 4586
AWS Shield 4606
AWS Diretor de segurança de rede Shield 4618
AWS Signatário 4621
AWS Entrando 4628
Mail Manager do Amazon Simple Email Service 4631
Amazon Simple Email Service v2 4649
Amazon Simple Workflow Service 4686
Amazon SimpleDB 4704
AWS SimSpace Tecelão 4708
AWS Gerenciamento de dispositivos Snow 4713
AWS Snowball 4718

Amazon SNS 4725
AWS Bancada de trabalho SQL 4736
Amazon SQS 4754
AWS Step Functions 4760
AWS Storage Gateway 4771
AWS Cadeia de suprimentos 4796
AWS Support 4805
AWS Support Aplicativo no Slack 4812
AWS Support Console 4816
AWS Support Planos 4820
AWS Sustentabilidade 4823
AWS Systems Manager 4825
AWS Systems Manager para SAP 4870
AWS Systems Manager GUI Connect 4878
AWS Systems Manager Gerenciador de incidentes 4881
AWS Contatos do Systems Manager Incident Manager 4890
AWS Configuração rápida do Systems Manager 4898
Tag Editor 4904
AWS Configurações fiscais 4906
AWS Construtor de rede Telco 4911
Amazon Textract 4921
Amazon Timestream 4928
Amazon Timestream InfluxDB 4939
AWS Tiros 4946
Amazon Transcribe 4949
AWS Transfer Family 4967
AWS Transformação 4981
Amazon Translate 4984
AWS Trusted Advisor 4991
AWS Notificações do usuário 5002
AWS Contatos de notificações do usuário 5011
AWS Assinaturas de usuário 5015
AWS Acesso verificado 5019
Amazon Verified Permissions 5021
Amazon VPC Lattice 5029
Serviços do Amazon VPC Lattice 5060

AWS WAF 5066
AWS WAF Regional 5080
AWS WAF VERSÃO 2 5096
AWS Ferramenta Well-Architected 5117
AWS Vime 5135
Amazon WorkDocs 5139
Amazon WorkLink 5151
Amazon WorkMail 5159
Fluxo de WorkMail mensagens da Amazon 5182
Amazon WorkSpaces 5185
Gerenciador WorkSpaces de aplicativos da Amazon 5207
AWS WorkSpaces Instâncias gerenciadas 5210
WorkSpaces Navegador Amazon Secure 5215
Amazon WorkSpaces Thin Client 5233
AWS X-Ray 5241
Recursos relacionados 5253
Acesso programático às informações de referência do serviço 5254
Definições de campo adicionais 5258
..... 5261

Referência

A Referência de Autorização de Serviço fornece uma lista das ações, recursos e chaves de condição que são suportadas por cada AWS serviço. Você pode especificar ações, recursos e chaves de condição nas políticas AWS Identity and Access Management (IAM) para gerenciar o acesso aos AWS recursos.

Conteúdo

- Ações, recursos e chaves de condição para AWS serviços
- Recursos relacionados

Ações, recursos e chaves de condição para AWS serviços

Cada AWS serviço pode definir ações, recursos e chaves de contexto de condição para uso nas políticas do IAM. Este tópico descreve como os elementos fornecidos para cada serviço estão documentados.

Cada tópico consiste em tabelas que fornecem a lista de ações, recursos e chaves de condição disponíveis.

A tabela de ações

A tabela Actions (Ações) lista todas as ações que você pode usar em um elemento `Action` de declaração de política do IAM. Nem todas as operações da API que são definidas por um serviço podem ser usadas como uma ação em uma política do IAM. Alguns serviços incluem ações somente de permissão que não correspondem diretamente a uma operação de API. Essas ações são indicadas com [permission only] (somente permissão). Use esta lista para determinar quais ações podem ser usadas em uma política do IAM. Para obter mais informações sobre os elementos `Action`, `Resource` ou `Condition`, consulte Referência de elementos de políticas JSON do IAM. As colunas Actions (Ações) e Description (Descrição) da tabela são autodescritivas.

- A coluna Access level (Nível de acesso) descreve como a ação é classificada (lista, leitura, gravação, gerenciamento de permissões ou marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre níveis de acesso, consulte Noções básicas sobre resumos de nível de acesso em resumos de política.

- A coluna Tipos de recursos indica se a ação é compatível com permissões em nível de recurso. Se a coluna estiver vazia, a ação não oferecerá suporte a permissões no nível do recurso e você deverá especificar todos os recursos ("*") em sua política. Se a coluna incluir um tipo de recurso, você poderá especificar o ARN do recurso no elemento `Resource` da política. Para obter mais informações sobre esse recurso, consulte essa linha na tabela Resource Types (Tipos de recursos). Todas as ações e recursos incluídos em uma declaração devem ser compatíveis entre si. Se você especificar um recurso que não é válido para a ação, qualquer solicitação para usar essa ação falhará e o `Effect` da declaração não será aplicado.

  Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você especificar um ARN de permissão no nível do recurso em uma instrução que esteja usando essa ação, ele deverá ser desse tipo. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um, mas não o outro.
- A coluna Condition keys (Chaves de condição) inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. As chaves de condição podem ser compatíveis com uma ação ou com uma ação e um recurso específico. Preste atenção se a chave está na mesma linha que um tipo de recurso específico. Essa tabela não inclui chaves de condição globais que estão disponíveis para qualquer ação ou em circunstâncias não relacionadas. Para obter mais informações sobre chaves de condição globais, consulte Chaves de contexto de condição globais da AWS.
- A coluna Ações dependentes inclui todas as permissões adicionais que você deve ter, além da permissão para a própria ação, para chamar a ação com êxito. Isso pode ser necessário se a ação acessar mais de um recurso.

  As ações dependentes não são necessárias em todos os cenários. Consulte a documentação específica do serviço para obter mais informações sobre como fornecer permissões granulares aos usuários.

A tabela de tipos de recursos

A tabela Resource Types (Tipos de recursos) lista todos os tipos de recursos que você pode especificar como um ARN no elemento `Resource`da política. Nem todo tipo de recurso pode ser especificado com cada ação. Alguns tipos de recursos funcionam apenas com determinadas ações. Se você especificar um tipo de recurso em uma instrução com uma ação que não oferece suporte a esse tipo de recurso, a instrução não permitirá o acesso. Para obter mais informações sobre o elemento `Resource`, consulte Elementos de políticas JSON do IAM: recurso.

- A coluna ARN especifica o nome do recurso da Amazon (ARN) que você deve usar para fazer referência a recursos desse tipo. As partes que são precedidas por um $ devem ser substituídas pelos valores reais de seu cenário. Por exemplo, se vir `$user-name` em um ARN, você deverá substituir essa string pelo nome do usuário efetivo ou por uma variável de política que contenha um nome do usuário. Para obter mais informações sobre ARNs, consulte IAM ARNs.
- A coluna Condition Keys (Chaves de condição) especifica chaves de contexto de condição que você pode incluir em uma declaração de política do IAM apenas quando esse recurso e uma ação compatível estão incluídos na declaração.

A tabela de chaves de condição

A tabela Condition Keys (Chaves de condição) lista todas as chaves de contexto de condição que você pode usar em um elemento `Condition` de declaração de política do IAM. Nem todas as chaves podem ser especificadas com cada ação ou recurso. Algumas chaves só funcionam com certos tipos de ações e recursos. Para obter mais informações sobre o elemento `Condition`, consulte Elementos de políticas JSON do IAM: condição.

- A coluna Type (Tipo) especifica o tipo de dados da chave de condição. Esse tipo de dados determina quais operadores de condição você pode usar para comparar valores na solicitação com os valores na declaração de política. Você deve usar um operador que seja apropriado para o tipo de dados. Se você usar um operador incorreto, a correspondência sempre falhará e a declaração da política nunca se aplicará.

  Se a coluna Type (Tipo) especificar uma “Lista de...” um dos tipos simples, você poderá usar várias chaves e valores em suas políticas. Faça isso usando prefixos de conjunto de condições com os operadores. Use o prefixo `ForAllValues` para especificar que todos os valores na solicitação devem corresponder a um valor na declaração de política. Use o prefixo `ForAnyValue` para especificar que pelo menos um valor na solicitação corresponde a um dos valores na declaração de política.

Tópicos

- Ações, recursos e chaves de condição do AWS Account Management
- Ações, recursos e chaves de condição para o AWS Activate
- Ações, recursos e chaves de condição para as operações de IA da Amazon
- Ações, recursos e chaves de condição do Alexa for Business

- Ações, recursos e chaves de condição para o AmazonMediaImport
- Ações, recursos e chaves de condição do AWS Amplify
- Ações, recursos e chaves de condição para o AWS Amplify Admin
- Ações, recursos e chaves de condição do AWS Amplify UI Builder
- Ações, recursos e chaves de condição do Apache Kafka para clusters APIs Amazon MSK
- Ações, recursos e chaves de condição do Amazon API Gateway
- Ações, recursos e chaves de condição do AWS App Mesh
- Ações, recursos e chaves de condição da pré-visualização do AWS App Mesh
- Ações, recursos e chaves de condição do AWS App Runner
- Ações, recursos e chaves de condição do AWS App Studio
- Ações, recursos e chaves de condição do AWS App2Container
- Ações, recursos e chaves de condição para o AWS AppConfig
- Ações, recursos e chaves de condição para o AWS AppFabric
- Ações, recursos e chaves de condição para a Amazon AppFlow
- Ações, recursos e chaves de condição para a Amazon AppIntegrations
- Ações, recursos e chaves de condição do AWS Application Auto Scaling
- Ações, recursos e chaves de condição do AWS Application Cost Profiler Service
- Ações, recursos e chaves de condição do Application Discovery Arsenal
- Ações, recursos e chaves de condição para o AWS Application DiscoveryService
- Ações, recursos e chaves de condição do AWS Application Migration Service
- Ações, recursos e chaves de condição para o Amazon Application Recovery Controller - Zonal Shift
- Ações, recursos e chaves de condição para o AWS Application Transformation Service
- Ações, recursos e chaves de condição para o Amazon AppStream 2.0
- Ações, recursos e chaves de condição para o AWS AppSync
- Ações, recursos e chaves de condição para a mudança de região ARC da Amazon
- Ações, recursos e chaves de condição do AWS Artifact
- Ações, recursos e chaves de condição do Amazon Athena
- Ações, recursos e chaves de condição do AWS Audit Manager
- Ações, recursos e chaves de condição para o Amazon Aurora DSQL

- Ações, recursos e chaves de condição do AWS Auto Scaling
- Ações, recursos e chaves de condição do AWS B2B Data Interchange
- Ações, recursos e chaves de condição do AWS Backup
- Ações, recursos e chaves de condição do AWS Backup Gateway
- Ações, recursos e chaves de condição para o AWS Backup Search
- Ações, recursos e chaves de condição do armazenamento do armazenamento do AWS Backup
- Ações, recursos e chaves de condição do AWS Batch
- Ações, recursos e chaves de condição do Amazon Bedrock
- Ações, recursos e chaves de condição para o Amazon Bedrock Agentcore
- Ações, recursos e chaves de condição para o AWS Billing
- Ações, recursos e chaves de condição para AWS Billing painéis de gerenciamento de custos
- Ações, recursos e chaves de condição para o AWS Billing And Cost Management Data Exports
- Ações, recursos e chaves de condição para AWS Billing And Cost Management Pricing Calculator
- Ações, recursos e chaves de condição para AWS Billing as ações recomendadas do And Cost Management
- Ações, recursos e chaves de condição para o AWS Billing Conductor
- Ações, recursos e chaves de condição do console do AWS Billing
- Ações, recursos e chaves de condição do Amazon Braket
- Ações, recursos e chaves de condição do AWS Budget Service
- Ações, recursos e chaves de condição para o AWS BugBust
- Ações, recursos e chaves de condição do AWS Certificate Manager
- Ações, recursos e chaves de condição do AWS Chatbot
- Ações, recursos e chaves de condição do Amazon Chime
- Ações, recursos e chaves de condição para o AWS Clean Rooms
- Ações, recursos e chaves de condição para o AWS Clean Rooms ML
- Ações, recursos e chaves de condição para a API do Nuvem AWS Control
- Ações, recursos e chaves de condição do Amazon Cloud Directory
- Ações, recursos e chaves de condição do Nuvem AWS Map
- Ações, recursos e chaves de condição do AWS Cloud9
- Ações, recursos e chaves de condição para o AWS CloudFormation

- Ações, recursos e chaves de condição para a Amazon CloudFront
- Ações, recursos e chaves de condição para a Amazon CloudFront KeyValueStore
- Ações, recursos e chaves de condição do AWS CloudHSM
- Ações, recursos e chaves de condição para a Amazon CloudSearch
- Ações, recursos e chaves de condição para o AWS CloudShell
- Ações, recursos e chaves de condição para o AWS CloudTrail
- Ações, recursos e chaves de condição para AWS CloudTrail dados
- Ações, recursos e chaves de condição para a Amazon CloudWatch
- Ações, recursos e chaves de condição para o Amazon CloudWatch Application Insights
- Ações, recursos e chaves de condição para Amazon CloudWatch Application Signals
- Ações, recursos e chaves de condição para a Amazon CloudWatch Evidently
- Ações, recursos e chaves de condição para o Amazon CloudWatch Internet Monitor
- Ações, recursos e chaves de condição para Amazon CloudWatch Logs
- Ações, recursos e chaves de condição para o Amazon CloudWatch Network Synthetic Monitor
- Ações, recursos e chaves de condição para o Amazon CloudWatch Observability Access Manager
- Ações, recursos e chaves de condição para o Amazon CloudWatch Observability Admin Service
- Ações, recursos e chaves de condição para AWS CloudWatch RUM
- Ações, recursos e chaves de condição para a Amazon CloudWatch Synthetics
- Ações, recursos e chaves de condição para o AWS CodeArtifact
- Ações, recursos e chaves de condição para a Amazon CodeCatalyst
- Ações, recursos e chaves de condição para o AWS CodeCommit
- Ações, recursos e chaves de condição para o AWS CodeConnections
- Ações, recursos e chaves de condição para o AWS CodeDeploy
- Ações, recursos e chaves de condição para o serviço AWS CodeDeploy seguro de comandos de host
- Ações, recursos e chaves de condição para a Amazon CodeGuru
- Ações, recursos e chaves de condição para o Amazon CodeGuru Profiler
- Ações, recursos e chaves de condição para o Amazon CodeGuru Reviewer
- Ações, recursos e chaves de condição para a Amazon CodeGuru Security
- Ações, recursos e chaves de condição para o AWS CodePipeline

- Ações, recursos e chaves de condição para o AWS CodeStar
- Ações, recursos e chaves de condição para AWS CodeStar conexões
- Ações, recursos e chaves de condição para AWS CodeStar notificações
- Ações, recursos e chaves de condição para a Amazon CodeWhisperer
- Ações, recursos e chaves de condição do Amazon Cognito Identity
- Ações, recursos e chaves de condição do Amazon Cognito Sync
- Ações, recursos e chaves de condição dos grupos de usuários do Amazon Cognito
- Ações, recursos e chaves de condição do Amazon Comprehend
- Ações, recursos e chaves de condição do Amazon Comprehend Medical
- Ações, recursos e chaves de condição do AWS Compute Optimizer
- Ações, recursos e chaves de condição do AWS Config
- Ações, recursos e chaves de condição do Amazon Connect Cases
- Ações, recursos e chaves de condição ao Amazon Connect Customer Profiles
- Ações, recursos e chaves de condição para campanhas externas do Amazon Connect
- Ações, recursos e chaves de condição para o Amazon Connect Voice ID
- Ações, recursos e chaves de condição do AWS Connector Service
- Ações, recursos e chaves de condição do AWS Management Console Mobile App
- Ações, recursos e chaves de condição para o AWS Consolidated Billing
- Ações, recursos e chaves de condição do AWS Control Catalog
- Ações, recursos e chaves de condição do AWS Control Tower
- Ações, recursos e chaves de condição do AWS Cost and Usage Report
- Ações, recursos e chaves de condição do AWS Cost Explorer Service
- Ações, recursos e chaves de condição do Hub de Otimização de Custos da AWS
- Ações, recursos e chaves de condição para o AWS Customer Verification Service
- Ações, recursos e chaves de condição do AWS Data Exchange
- Ações, recursos e chaves de condição do Amazon Data Lifecycle Manager
- Ações, recursos e chaves de condição do AWS Data Pipeline
- Ações, recursos e chaves de condição do AWS Database Migration Service
- Ações, recursos e chaves de condição do Database Query Metadata Service
- Ações, recursos e chaves de condição para o AWS DataSync

- Ações, recursos e chaves de condição para a Amazon DataZone
- Ações, recursos e chaves de condição do AWS Deadline Cloud
- Ações, recursos e chaves de condição para o AWS DeepComposer
- Ações, recursos e chaves de condição para o AWS DeepRacer
- Ações, recursos e chaves de condição do Amazon Detective
- Ações, recursos e chaves de condição do AWS Device Farm
- Ações, recursos e chaves de condição para o Amazon DevOps Guru
- Ações, recursos e chaves de condição para as Ferramentas de diagnóstico da AWS
- Ações, recursos e chaves de condição do AWS Direct Connect
- Ações, recursos e chaves de condição do AWS Directory Service
- Ações, recursos e chaves de condição do AWS Directory Service Data
- Ações, recursos e chaves de condição do Amazon DocumentDB Elastic Clusters
- Ações, recursos e chaves de condição do Amazon DynamoDB
- Ações, recursos e chaves de condição do Amazon DynamoDB Accelerator (DAX)
- Ações, recursos e chaves de condição para o Amazon EC2 Auto Scaling
- Ações, recursos e chaves de condição para o Amazon EC2 Image Builder
- Ações, recursos e chaves de condição para o Amazon EC2 Instance Connect
- Ações, recursos e chaves de condição do Amazon EKS Auth
- Ações, recursos e chaves de condição do AWS Elastic Beanstalk
- Ações, recursos e chaves de condição do Amazon Elastic Block Store
- Ações, recursos e chaves de condição do Amazon Elastic Container Registry
- Ações, recursos e chaves de condição para o Amazon Elastic Container Registry Public
- Ações, recursos e chaves de condição do Amazon Elastic Container Service
- Ações, recursos e chaves de condição para AWS Elastic Disaster Recovery
- Ações, recursos e chaves de condição do Amazon Elastic File System
- Ações, recursos e chaves de condição para o Amazon Elastic Kubernetes Service
- Ações, recursos e chaves de condição para o AWS Elastic Load Balancing
- Ações, recursos e chaves de condição do AWS Elastic Load Balancing V2
- Ações, recursos e chaves de condição para o Amazon Elastic MapReduce
- Ações, recursos e chaves de condição do Amazon Elastic Transcoder

- Ações, recursos e chaves de condição para o Amazon Elastic VMware Service
- Ações, recursos e chaves de condição para a Amazon ElastiCache
- Ações, recursos e chaves de condição do AWS Elemental Appliances and Software
- Ações, recursos e chaves de condição do AWS Elemental Appliances and Software Activation Service
- Ações, recursos e chaves de condição para AWS Elemental MediaConnect
- Ações, recursos e chaves de condição para AWS Elemental MediaConvert
- Ações, recursos e chaves de condição para AWS Elemental MediaLive
- Ações, recursos e chaves de condição para AWS Elemental MediaPackage
- Ações, recursos e chaves de condição para o AWS Elemental MediaPackage V2
- Ações, recursos e chaves de condição para AWS Elemental VOD MediaPackage
- Ações, recursos e chaves de condição para AWS Elemental MediaStore
- Ações, recursos e chaves de condição para AWS Elemental MediaTailor
- Ações, recursos e chaves de condição para o AWS Elemental Support Cases
- Ações, recursos e chaves de condição para o AWS Elemental Support Content
- Ações, recursos e chaves de condição para o Amazon EMR no EKS (contêineres EMR)
- Ações, recursos e chaves de condição para o Amazon EMR Servereless
- Ações, recursos e chaves de condição para mensagens de usuário AWS final, SMS e voz V2
- Ações, recursos e chaves de condição do AWS End User Messaging Social
- Ações, recursos e chaves de condição do AWS Entity Resolution
- Ações, recursos e chaves de condição para a Amazon EventBridge
- Ações, recursos e chaves de condição para Amazon EventBridge Pipes
- Ações, recursos e chaves de condição para o Amazon EventBridge Scheduler
- Ações, recursos e chaves de condição para Amazon EventBridge Schemas
- Ações, recursos e chaves de condição para o AWS Fault Injection Service
- Ações, recursos e chaves de condição para a Amazon FinSpace
- Ações, recursos e chaves de condição para a FinSpace API da Amazon
- Ações, recursos e chaves de condição do AWS Firewall Manager
- Ações, recursos e chaves de condição do Amazon Forecast
- Ações, recursos e chaves de condição do Amazon Fraud Detector

- Ações, recursos e chaves de condição para o nível gratuito da AWS
- Ações, recursos e chaves de condição do Amazon FreeRTOS
- Ações, recursos e chaves de condição para a Amazon FSx
- Ações, recursos e chaves de condição para GameLift servidores Amazon
- Ações, recursos e chaves de condição para o Amazon GameLift Streams
- Ações, recursos e chaves de condição do AWS Global Accelerator
- Ações, recursos e chaves de condição do AWS Glue
- Ações, recursos e chaves de condição para AWS Glue DataBrew
- Ações, recursos e chaves de condição do AWS Ground Station
- Ações, recursos e chaves de condição para a Amazon GroundTruth Labeling
- Ações, recursos e chaves de condição para a Amazon GuardDuty
- Ações, recursos e chaves de condição para AWS Health APIs and Notifications
- Ações, recursos e chaves de condição para o AWS HealthImaging
- Ações, recursos e chaves de condição para o AWS HealthLake
- Ações, recursos e chaves de condição para o AWS HealthOmics
- Ações, recursos e chaves de condição do Amazon Honeycode
- Ações, recursos e chaves de condição do AWS IAM Access Analyzer
- Ações, recursos e chaves de condição para o AWS IAM Identity Center
- Ações, recursos e chaves de condição para o diretório AWS do IAM Identity Center
- Ações, recursos e chaves de condição para o serviço OIDC do Centro de Identidade do AWS IAM
- Ações, recursos e chaves de condição para o AWS Identity and Access Management (IAM)
- Ações, recursos e chaves de condição para o AWS Identity and Access Management Roles Anywhere
- Ações, recursos e chaves de condição do AWS Identity Store
- Ações, recursos e chaves de condição do AWS Identity Store Auth
- Ações, recursos e chaves de condição para o AWS Identity Sync
- Ações, recursos e chaves de condição do AWS Import Export Disk Service
- Ações, recursos e chaves de condição do Amazon Inspector
- Ações, recursos e chaves de condição para Amazon Inspecto2
- Ações, recursos e chaves de condição para a Amazon InspectorScan

- Ações, recursos e chaves de condição do Amazon Interactive Video Service
- Ações, recursos e chaves de condição do chat do Amazon Interactive Video Service
- Ações, recursos e chaves de condição para o AWS Invoicing Service
- Ações, recursos e chaves de condição do AWS IoT 1-Click
- Ações, recursos e chaves de condição do AWS IoT Analytics
- Ações, recursos e chaves de condição do AWS IoT Core Device Advisor
- Ações, recursos e chaves de condição do AWS IoT Device Tester
- Ações, recursos e chaves de condição do AWS IoT Events
- Ações, recursos e chaves de condição do AWS IoT Fleet Hub for Device Management
- Ações, recursos e chaves de condição para AWS IoT FleetWise
- Ações, recursos e chaves de condição do AWS IoT Greengrass
- Ações, recursos e chaves de condição para o AWS IoT Greengrass V2
- Ações, recursos e chaves de condição para trabalhos de AWS IoT DataPlane
- Ações, recursos e chaves de condição para integrações gerenciadas de AWS IoT
- Ações, recursos e chaves de condição para AWS IoT SiteWise
- Ações, recursos e chaves de condição para AWS IoT TwinMaker
- Ações, recursos e chaves de condição do AWS IoT Wireless
- Ações, recursos e chaves de condição do AWS IQ
- Ações, recursos e chaves de condição do AWS IQ Permissions
- Ações, recursos e chaves de condição do Amazon Kendra
- Ações, recursos e chaves de condição para o Amazon Kendra Intelligent Ranking
- Ações, recursos e chaves de condição do Amazon Keyspaces (for Apache Cassandra)
- Ações, recursos e chaves de condição do Amazon Kinesis Analytics
- Ações, recursos e chaves de condição do Amazon Kinesis Analytics V2
- Ações, recursos e chaves de condição do Amazon Kinesis Data Streams
- Ações, recursos e chaves de condição do Amazon Kinesis Firehose
- Ações, recursos e chaves de condição do Amazon Kinesis Video Streams
- Ações, recursos e chaves de condição do AWS Lake Formation
- Ações, recursos e chaves de condição do AWS Lambda
- Ações, recursos e chaves de condição para o AWS Launch Wizard

- Ações, recursos e chaves de condição do Amazon Lex
- Ações, recursos e chaves de condição do Amazon Lex V2
- Ações, recursos e chaves de condição do AWS License Manager
- Ações, recursos e chaves de condição para o AWS License Manager Linux Subscriptions Manager
- Ações, recursos e chaves de condição para o AWS License Manager User Subscriptions
- Ações, recursos e chaves de condição do Amazon Lightsail
- Ações, recursos e chaves de condição para o Amazon Location
- Ações, recursos e chaves de condição para Amazon Location Service Maps
- Ações, recursos e chaves de condição para Amazon Location Service Places
- Ações, recursos e chaves de condição para Amazon Location Service Routes
- Ações, recursos e chaves de condição do Amazon Lookout for Equipment
- Ações, recursos e chaves de condição do Amazon Lookout for Metrics
- Ações, recursos e chaves de condição do Amazon Lookout for Vision
- Ações, recursos e chaves de condição do Amazon Machine Learning
- Ações, recursos e chaves de condição do Amazon Macie
- Ações, recursos e chaves de condição do Application Testing do AWS Mainframe Modernization
- Ações, recursos e chaves de condição para o AWS Mainframe Modernization Service
- Ações, recursos e chaves de condição do Amazon Managed Blockchain
- Ações, recursos e chaves de condição do Amazon Managed Blockchain Query
- Ações, recursos e chaves de condição para o Amazon Managed Grafana
- Ações, recursos e chaves de condição para o Amazon Managed Service for Prometheus
- Ações, recursos e chaves de condição do Amazon Managed Streaming for Apache Kafka
- Ações, recursos e chaves de condição do Amazon Managed Streaming for Kafka Connect
- Ações, recursos e chaves de condição para o Amazon Managed Workflows for Apache Airflow
- Ações, recursos e chaves de condição para o AWS Marketplace
- Ações, recursos e chaves de condição do AWS Marketplace Catalog
- Ações, recursos e chaves de condição do AWS Marketplace Commerce Analytics Service
- Ações, recursos e chaves de condição do Serviço de Implantação da AWS Marketplace
- Ações, recursos e chaves de condição do AWS Marketplace Discovery
- Ações, recursos e chaves de condição do AWS Marketplace Entitlement Service

- Ações, recursos e chaves de condição do AWS Marketplace Image Building Service
- Ações, recursos e chaves de condição do AWS Marketplace Management Portal
- Ações, recursos e chaves de condição do AWS Marketplace Metering Service
- Ações, recursos e chaves de condição do AWS Marketplace Private Marketplace
- Ações, recursos e chaves de condição do AWS Marketplace Procurement Systems Integration
- Ações, recursos e chaves de condição do AWS Marketplace Reporting
- Ações, recursos e chaves de condição do AWS Marketplace Seller Reporting
- Ações, recursos e chaves de condição do AWS Marketplace Vendor Insights
- Ações, recursos e chaves de condição do Amazon Mechanical Turk
- Ações, recursos e chaves de condição para o Amazon MemoryDB
- Ações, recursos e chaves de condição do Serviço de entrega de mensagens da Amazon
- Ações, recursos e chaves de condição do Amazon Message Gateway Service
- Ações, recursos e chaves de condição para o AWS Microservice Extractor for .NET
- Ações, recursos e chaves de condição para créditos do Programa de Aceleração da Migração da AWS
- Ações, recursos e chaves de condição do AWS Migration Hub
- Ações, recursos e chaves de condição do AWS Migration Hub Orchestrator
- Ações, recursos e chaves de condição do AWS Migration Hub Refactor Spaces
- Ações, recursos e chaves de condição para o AWS Migration Hub Strategy Recommendations
- Ações, recursos e chaves de condição do Amazon Mobile Analytics
- Ações, recursos e chaves de condição para o Amazon Monitron
- Ações, recursos e chaves de condição do Amazon MQ
- Ações, recursos e chaves de condição para aprovação multipartidária
- Ações, recursos e chaves de condição do Amazon Neptune
- Ações, recursos e chaves de condição do Amazon Neptune Analytics
- Ações, recursos e chaves de condição do AWS Network Firewall
- Ações, recursos e chaves de condição para o Network Flow Monitor
- Ações, recursos e chaves de condição para o AWS Network Manager
- Ações, recursos e chaves de condição para o AWS Network Manager Chat
- Ações, recursos e chaves de condição do Amazon Nimble Studio
- Ações, recursos e chaves de condição do Amazon One Enterprise

- Ações, recursos e chaves de condição para a Amazon OpenSearch
- Ações, recursos e chaves de condição para o Amazon OpenSearch Inestion
- Ações, recursos e chaves de condição para o Amazon OpenSearch Serverless
- Ações, recursos e chaves de condição para o Amazon OpenSearch Service
- Ações, recursos e chaves de condição para o AWS OpsWorks
- Ações, recursos e chaves de condição para o gerenciamento de AWS OpsWorks configuração
- Ações, recursos e chaves de condição do AWS Organizations
- Ações, recursos e chaves de condição do AWS Outposts
- Ações, recursos e chaves de condição do AWS Panorama
- Ações, recursos e chaves de condição do AWS Parallel Computing Service
- Ações, recursos e chaves de condição para o gerenciamento de contas da Central de Parceiros da AWS
- Ações, recursos e chaves de condição para o AWS Partner Central Selling
- Ações, recursos e chaves de condição para Criptografia de Pagamento da AWS
- Ações, recursos e chaves de condição para o AWS Payments
- Ações, recursos e chaves de condição do AWS Performance Insights
- Ações, recursos e chaves de condição do Amazon Personalize
- Ações, recursos e chaves de condição do Amazon Pinpoint
- Ações, recursos e chaves de condição do Serviço de e-mail do Amazon Pinpoint
- Ações, recursos e chaves de condição do Serviço de SMS e voz do Amazon Pinpoint
- Ações, recursos e chaves de condição do Amazon Polly
- Ações, recursos e chaves de condição do AWS Price List
- Ações, recursos e chaves de condição para o AWS Private CA Connector for Active Directory
- Ações, recursos e chaves de condição do AWS Private CA Connector para SCEP
- Ações, recursos e chaves de condição para a AWS Private Certificate Authority
- Ações, recursos e chaves de condição para o AWS PrivateLink
- Ações, recursos e chaves de condição do AWS Proton
- Ações, recursos e chaves de condição do console do AWS Purchase Orders
- Ações, recursos e chaves de condição do Amazon Q
- Ações, recursos e chaves de condição do Amazon Q Business
- Ações, recursos e chaves de condição para aplicações do Q do Amazon Q Business

- Ações, recursos e chaves de condição para o Amazon Q Developer
- Ações, recursos e chaves de condição do Amazon Q in Connect
- Ações, recursos e chaves de condição do Amazon QLDB
- Ações, recursos e chaves de condição para a Amazon QuickSight
- Ações, recursos e chaves de condição da API Data do Amazon RDS
- Ações, recursos e chaves de condição para autenticação do IAM do Amazon RDS
- Ações, recursos e chaves de condição para o AWS Recycle Bin
- Ações, recursos e chaves de condição do Amazon Redshift
- Ações, recursos e chaves de condição da API Data do Amazon Redshift
- Ações, recursos e chaves de condição para o Amazon Redshift Serverless
- Ações, recursos e chaves de condição do Amazon Rekognition
- Ações, recursos e chaves de condição para o AWS RePost Private
- Ações, recursos e chaves de condição para o AWS Resilience Hub
- Ações, recursos e chaves de condição do AWS Resource Access Manager (RAM)
- Ações, recursos e chaves de condição do AWS Resource Explorer
- Ações, recursos e chaves de condição da API de marcação de resource groups da Amazon
- Ações, recursos e chaves de condição do AWS Resource Groups
- Ações, recursos e chaves de condição do Amazon RHEL Knowledgebase Portal
- Ações, recursos e chaves de condição para o AWS RoboMaker
- Ações, recursos e chaves de condição do Amazon Route 53
- Ações, recursos e chaves de condição para domínios do Amazon Route 53
- Ações, recursos e chaves de condição do Amazon Route 53 Profiles
- Ações, recursos e chaves de condição do Amazon Route 53 Recovery Cluster
- Ações, recursos e chaves de condição do Amazon Route 53 Recovery Controls
- Ações, recursos e chaves de condição para o Amazon Route 53 Recovery Readiness
- Ações, recursos e chaves de condição do Amazon Route 53 Resolver
- Ações, recursos e chaves de condição do Amazon S3 Express
- Ações, recursos e chaves de condição do Amazon S3 Glacier
- Ações, recursos e chaves de condição do Amazon S3 Object Lambda
- Ações, recursos e chaves de condição do Amazon S3 on Outposts

- Ações, recursos e chaves de condição para tabelas do Amazon S3
- Ações, recursos e chaves de condição para Amazon S3 Vectors
- Ações, recursos e chaves de condição para o assistente de ciência SageMaker de dados da Amazon
- Ações, recursos e chaves de condição para as capacidades SageMaker geoespaciais da Amazon
- Ações, recursos e chaves de condição para a Amazon SageMaker com MLflow
- Ações, recursos e chaves de condição do AWS Savings Plans
- Ações, recursos e chaves de condição do AWS Secrets Manager
- Ações, recursos e chaves de condição do AWS Security Hub
- Ações, recursos e chaves de condição para Resposta a Incidentes AWS de Segurança
- Ações, recursos e chaves de condição do Amazon Security Lake
- Ações, recursos e chaves de condição do AWS Server Migration Service
- Ações, recursos e chaves de condição do AWS Serverless Application Repository
- Ações, recursos e chaves de condição para AWS Service - Oracle Database@AWS
- Ações, recursos e chaves de condição do AWS Service Catalog
- Ações, recursos e chaves de condição do AWS Serviço para gerenciar recursos de experiência AWS Management Console do usuário.
- Ações, recursos e chaves de condição para o serviço da AWS que fornece redes privadas gerenciadas
- Ações, recursos e chaves de condição do Service Quotas
- Ações, recursos e chaves de condição do Amazon SES
- Ações, recursos e chaves de condição do AWS Shield
- Ações, recursos e chaves de condição para o diretor de segurança de rede AWS Shield
- Ações, recursos e chaves de condição para o AWS Signer
- Ações, recursos e chaves de condição do AWS Signin
- Ações, recursos e chaves de condição do Amazon Simple Email Service para Mail Manager
- Ações, recursos e chaves de condição do Amazon Simple Email Service v2
- Ações, recursos e chaves de condição do Amazon Simple Workflow Service
- Ações, recursos e chaves de condição do Amazon SimpleDB
- Ações, recursos e chaves de condição para AWS SimSpace Weaver
- Ações, recursos e chaves de condição para o AWS Snow Device Management

- Ações, recursos e chaves de condição do AWS Snowball
- Ações, recursos e chaves de condição do Amazon SNS
- Ações, recursos e chaves de condição para o AWS SQL Workbench
- Ações, recursos e chaves de condição do Amazon SQS
- Ações, recursos e chaves de condição do AWS Step Functions
- Ações, recursos e chaves de condição do AWS Storage Gateway
- Ações, recursos e chaves de condição do AWS Supply Chain
- Ações, recursos e chaves de condição para o AWS Support
- Ações, recursos e chaves de condição do AWS Support App no Slack
- Ações, recursos e chaves de condição do console do AWS Support
- Ações, recursos e chaves de condição do AWS Support Plans
- Ações, recursos e chaves de condição para o AWS Sustainability
- Ações, recursos e chaves de condição do AWS Systems Manager
- Ações, recursos e chaves de condição do AWS Systems Manager para SAP
- Ações, recursos e chaves de condição do AWS Systems Manager GUI Connect
- Ações, recursos e chaves de condição do AWS Systems Manager Incident Manager
- Ações, recursos e chaves de condição do AWS Systems Manager Incident Manager Contacts
- Ações, recursos e chaves de condição da Configuração Rápida do AWS Systems Manager
- Ações, recursos e chaves de condição para o Tag Editor
- Ações, recursos e chaves de condição para o AWS Tax Settings
- Ações, recursos e chaves de condição do AWS Telco Network Builder
- Ações, recursos e chaves de condição do Amazon Textract
- Ações, recursos e chaves de condição para o Amazon Timestream
- Ações, recursos e chaves de condição do Amazon Timestream InfluxDB
- Ações, recursos e chaves de condição do AWS Tiros
- Ações, recursos e chaves de condição do Amazon Transcribe
- Ações, recursos e chaves de condição do AWS Transfer Family
- Ações, recursos e chaves de condição para AWS Transform
- Ações, recursos e chaves de condição do Amazon Translate
- Ações, recursos e chaves de condição do AWS Trusted Advisor

- Ações, recursos e chaves de condição do AWS User Notifications
- Ações, recursos e chaves de condição para AWS User Notifications Contacts
- Ações, recursos e chaves de condição do AWS User Subscriptions
- Ações, recursos e chaves de condição para o AWS Verified Access
- Ações, recursos e chaves de condição do Amazon Verified Permissions
- Ações, recursos e chaves de condição do Amazon VPC Lattice
- Ações, recursos e chaves de condição do Amazon VPC Lattice Services
- Ações, recursos e chaves de condição para o AWS WAF
- Ações, recursos e chaves de condição para o AWS WAF Regional
- Ações, recursos e chaves de condição para o AWS WAF V2
- Ações, recursos e chaves de condição do AWS Well-Architected Tool
- Ações, recursos e chaves de condição para o AWS Wickr
- Ações, recursos e chaves de condição para a Amazon WorkDocs
- Ações, recursos e chaves de condição para a Amazon WorkLink
- Ações, recursos e chaves de condição para a Amazon WorkMail
- Ações, recursos e chaves de condição para o Amazon WorkMail Message Flow
- Ações, recursos e chaves de condição para a Amazon WorkSpaces
- Ações, recursos e chaves de condição para o Amazon WorkSpaces Application Manager
- Ações, recursos e chaves de condição para instâncias AWS WorkSpaces gerenciadas
- Ações, recursos e chaves de condição para o Amazon WorkSpaces Secure Browser
- Ações, recursos e chaves de condição para o Amazon WorkSpaces Thin Client
- Ações, recursos e chaves de condição do AWS X-Ray

Ações, recursos e chaves de condição do AWS Account Management

AWS O gerenciamento de contas (prefixo do serviço:`account`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.

- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Account Management
- Tipos de recursos definidos pelo AWS Account Management
- Chaves de condição para o AWS Account Management

Ações definidas pelo AWS Account Management

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptPrimaryEmailUpdate	Concede permissão para aceitar o processo de atualização do endereço de e-mail principal de uma conta	Gravar	accountInOrganization		
				account:EmailTargetDomain	
CloseAccount [somente permissão]	Concede permissão para fechar uma conta	Gravar	account		
DeleteAlternateContact	Concede permissão para excluir os contatos alternativos de uma conta	Write	account		
			accountInOrganization		
				account:AlternateContactTypes	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisableRegion	Concede permissão para desabilitar o uso de uma região	Write	account		
			accountInOrganization		
				account:TargetRegion	
EnableRegion	Concede permissão para habilitar o uso de uma região	Gravar	account		
			accountInOrganization		
				account:TargetRegion	
GetAccountInformation	Concede permissão para recuperar as informações de conta de uma conta	Leitura	account		
			accountInOrganization		
GetAlternateContact	Concede permissão para recuperar os contatos alternativos de uma conta	Leitura	account		
			accountInOrganization		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				account:AlternateContactTypes	
GetContactInformation	Concede permissão para recuperar as principais informações de contato de uma conta	Leitura	account		
			accountInOrganization		
GetPrimaryEmail	Concede permissão para recuperar o endereço de e-mail principal de uma conta	Leitura	accountInOrganization		
GetRegionOptStatus	Concede permissão para obter o status de aceitação de uma região	Leitura	account		
			accountInOrganization		
				account:TargetRegion	
ListRegions	Concede permissão para listar as regiões disponíveis	Lista	account		
			accountInOrganization		
PutAccountName	Concede permissão para atualizar o nome de uma conta	Gravar	account		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			accountInOrganization		
PutAlternateContact	Concede permissão para modificar os contatos alternativos de uma conta	Gravar	account		
			accountInOrganization		
				account:AlternateContactTypes	
PutContactInformation	Concede permissão para atualizar as principais informações de contato de uma conta	Gravar	account		
			accountInOrganization		
StartPrimaryEmailUpdate	Concede permissão para iniciar o processo de atualização do endereço de e-mail principal de uma conta	Gravar	accountInOrganization		
				account:EmailTargetDomain	

Tipos de recursos definidos pelo AWS Account Management

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações

identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
account	`arn:${Partition}:account::${Account}:account`	
accountInOrganization	`arn:${Partition}:account::${ManagementAccountId}:account/o-${OrganizationId}/${MemberAccountId}`	

Chaves de condição para o AWS Account Management

AWS O gerenciamento de contas define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
account:AccountResourceOrgPaths	Filtra o acesso por caminho de recurso para uma conta em uma organização	ArrayOfString
account:AccountResourceOrgTags/${TagKey}	Filtra o acesso por etiquetas de recurso para uma conta em uma organização	String

Chaves de condição	Descrição	Tipo
account:AlternateContactTypes	Filtra o acesso por tipos de contato alternativos	ArrayOfString
account:EmailTargetDomain	Filtra o acesso por domínio de e-mail do endereço de e-mail de destino	String
account:TargetRegion	Filtra o acesso por uma lista de regiões. Habilita ou desabilita todas as regiões especificadas aqui	String

Ações, recursos e chaves de condição para o AWS Activate

AWS Activate (prefixo do serviço:`activate`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Activate
- Tipos de recursos definidos pelo AWS Activate
- Chaves de condição do AWS Activate

Ações definidas pelo AWS Activate

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateForm	Concede permissão para enviar um formulário de inscrição do Activate	Gravar			
GetAccountContact	Concede permissão para obter as informações de Conta da AWS contato	Leitura			
GetContentInfo	Concede permissão para obter publicações técnicas do Activate e oferecer informações	Leitura			
GetCosts	Concede permissão para obter as informações AWS de custo	Leitura			
GetCredits	Concede permissão para obter as informações AWS de crédito	Leitura			
GetMemberInfo	Concede permissão para obter as informações do membro Activate	Read			
GetProgram	Concede permissão para obter um programa Activate	Read			
PutMemberInfo	Concede permissão para criar ou atualizar as informações do membro Activate	Write			

Tipos de recursos definidos pelo AWS Activate

AWS O Activate não suporta a especificação de um ARN de recurso `Resource` no elemento de uma declaração de política do IAM. Para permitir o acesso ao AWS Activate, especifique `"Resource": "*"` na política.

Chaves de condição do AWS Activate

O Activate não possui chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento de instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para as operações de IA da Amazon

O Amazon AI Operations (prefixo do serviço:`aiops`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon AI Operations
- Tipos de recursos definidos pelas operações de IA da Amazon
- Chaves de condição para operações de IA da Amazon

Ações definidas pela Amazon AI Operations

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateInvestigation	Concede permissão para criar uma nova investigação no grupo de investigação especificado	Gravar	investigation-group*		kms:Decrypt kms:GenerateDataKey sts:SetContext
CreateInvestigationEvent	Concede permissão para criar um novo evento de investigação no grupo de investigação especificado	Gravar	investigation-group*		cloudwatch:DescribeAlarmHistory cloudwatch:DescribeAlarms cloudwatch:GetInsightRuleReport cloudwatch:GetMetricData kms:Decrypt kms:GenerateDataKey

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					logs:GetQueryResults sts:SetContext

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateInvestigationGroup	Concede permissão para criar um novo grupo de investigação	Gravar		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

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					sso:PutApplicationAssignmentConfiguration sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant sso:TagResource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateInvestigationResource	Concede permissão para criar um recurso de investigação no grupo de investigação especificado	Gravar	investigation-group*		cloudwatch:DescribeAlarmHistory cloudwatch:DescribeAlarms cloudwatch:GetInsightRuleReport cloudwatch:GetMetricData kms:GenerateDataKey logs:GetQueryResults
DeleteInvestigation	Concede permissão para excluir uma investigação no grupo de investigação especificado	Gravar	investigation-group*		sts:SetContext

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteInvestigationGroup	Concede permissão para excluir o grupo de investigação especificado	Gravar	investigation-group*		sso:DeleteApplication
DeleteInvestigationGroupPolicy	Concede permissão para excluir a política do grupo de investigação anexada a um grupo de investigação	Gravar	investigation-group*		
GetInvestigation	Concede permissão para recuperar uma investigação no grupo de investigação especificado	Leitura	investigation-group*		
GetInvestigationEvent	Concede permissão para recuperar um evento de investigação no grupo de investigação especificado	Leitura	investigation-group*		kms:Decrypt
GetInvestigationGroup	Concede permissão para recuperar o grupo de investigação especificado	Leitura	investigation-group*		
GetInvestigationGroupPolicy	Concede permissão para recuperar a política do grupo de investigação anexada a um grupo de investigação	Leitura	investigation-group*		
GetInvestigationResource	Concede permissão para recuperar um recurso de investigação no grupo de investigação especificado	Leitura	investigation-group*		kms:Decrypt

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListInvestigationEvents	Concede permissão para listar todos os eventos de investigação no grupo de investigação especificado	Lista	investigation-group*		
ListInvestigationGroups	Concede permissão para listar todos os grupos de investigação ao Conta da AWS fazer a solicitação	Lista			
ListInvestigations	Concede permissão para listar todas as investigações que estão no grupo de investigação especificado	Lista	investigation-group*		
ListTagsForResource	Concede permissão para listar as etiquetas para o recurso especificado	Lista	investigation-group*		
PutInvestigationGroupPolicy	Concede permissão à política create/update do grupo de investigação anexada a um grupo de investigação	Gravar	investigation-group*		
TagResource	Concede permissão para adicionar ou atualizar as etiquetas especificadas no recurso especificado	Tags	investigation-group*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover as etiquetas especificadas do recurso especificado	Tags	investigation-group*		
				aws:TagKeys	
UpdateInvestigation	Concede permissão para atualizar uma investigação no grupo de investigação especificado	Gravar	investigation-group*		kms:Decrypt kms:GenerateDataKey sts:SetContext
UpdateInvestigationEvent	Concede permissão para atualizar um evento de investigação no grupo de investigação especificado	Gravar	investigation-group*		kms:Decrypt kms:GenerateDataKey sts:SetContext

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateInvestigationGroup	Concede permissão para atualizar o grupo de investigação especificado	Gravar	investigation-group*		cloudtrail:DescribeTrails iam:PassRole kms:Decrypt kms:DescribeKey kms:GenerateDataKey sso:CreateApplication sso:DeleteApplication sso:PutApplicationAccessScope sso:PutApplicationAssignmen

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					tConfiguration sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant sso:TagResource
ValidateInvestigationGroup	Concede permissão para validar o grupo de investigação especificado	Leitura	investigation-group*		

Tipos de recursos definidos pelas operações de IA da Amazon

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
investigation-group	`arn:${Partition}:aiops:${Region}:${Account}:investigation-group/${InvestigationGroupId}`	aws:ResourceTag/${TagKey}

Chaves de condição para operações de IA da Amazon

As operações de IA da Amazon definem as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Alexa for Business

O Alexa for Business (prefixo do serviço: `a4b`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Alexa for Business
- Tipos de recursos definidos pelo Alexa for Business
- Chaves de condição do Alexa for Business

Ações definidas pelo Alexa for Business

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de

condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ApproveSkill	Concede permissão para associar uma habilidade à organização sob a responsabilidade do cliente Conta da AWS	Write			
AssociateContactWithAddressBook	Concede permissão para associar um contato a um determinado catálogo de endereços	Write	addressbook*		
			contact*		
AssociateDeviceWithNetworkProfile	Concede permissão para associar um dispositivo ao perfil de rede especificado	Write	device*		
			networkprofile*		
AssociateDeviceWithRoom	Concede permissão para associar um dispositivo a uma determinada sala	Write	device*		
			room*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateSkillGroupWithRoom	Concede permissão para associar o grupo de skills a uma determinada sala	Write	room* skillgroup*		
AssociateSkillWithSkillGroup	Concede permissão para associar uma skill a um grupo de skills	Write	skillgroup*		
AssociateSkillWithUsers	Concede permissão para disponibilizar uma skill privada para usuários inscritos habilitarem em seus dispositivos	Write			
CompleteRegistration [somente permissão]	Concede permissão para concluir a operação de registro de um dispositivo Alexa	Write			
CreateAddressBook	Concede permissão para criar um catálogo de endereços com os detalhes especificados	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateBusinessReportSchedule	Concede permissão para criar uma programação recorrente para relatórios de uso a serem entregues no local S3 especificado com um intervalo diário ou semanal especificado	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConferenceProvider	Concede permissão para adicionar um novo provedor de conferência abaixo do do usuário Conta da AWS	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateContact	Concede permissão para criar um contato com os detalhes especificados	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateGatewayGroup	Concede permissão para criar um grupo de gateways com os detalhes especificados	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateNetworkProfile	Concede permissão para criar um perfil de rede com os detalhes especificados	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfile	Concede permissão para criar um novo perfil	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRoom	Concede permissão para criar uma sala com os detalhes especificados	Write	profile*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSkillGroup	Concede permissão para criar um grupo de skills com determinado nome e descrição	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateUser	Concede permissão para criar um usuário	Write	user*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAddressBook	Concede permissão para excluir um catálogo de endereços pelo ARN do catálogo de endereços	Write	addressbook*		
DeleteBusinessReportSchedule	Concede permissão para excluir a programação de entrega de relatório recorrente com o ARN da programação especificada	Write	schedule*		
DeleteConferenceProvider	Concede permissão para excluir um provedor de conferência	Write	conferenceprovider*		
DeleteContact	Concede permissão para excluir um contato pelo ARN do contato	Write	contact*		
DeleteDevice	Concede permissão para remover um dispositivo do Alexa For Business	Write	device*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteDeviceUsageData	Concede permissão para excluir todo o histórico anterior do dispositivo de dados de entrada de voz e dados de resposta associados	Write	device*		
DeleteGatewayGroup	Concede permissão para excluir um grupo de gateway	Write	gatewaygroup*		
DeleteNetworkProfile	Concede permissão para excluir um perfil de rede pelo ARN do perfil de rede	Write	networkprofile*		
DeleteProfile	Concede permissão para excluir um perfil pelo ARN do perfil	Write	profile*		
DeleteRoom	Concede permissão para excluir uma sala	Write	room*		
DeleteRoomSkillParameter	Concede permissão para excluir um parâmetro de uma skill e uma sala	Write	room*		
DeleteSkillAuthorization	Concede permissão para desvincular uma conta de terceiros de uma skill	Write	room*		
DeleteSkillGroup	Concede permissão para excluir um grupo de skills com o ARN do grupo de skills	Write	skillgroup*		
DeleteUser	Concede permissão para excluir um usuário	Write	user*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateContactFromAddressBook	Concede permissão para desassociar um contato de um determinado catálogo de endereços	Write	addressbook*		
			contact*		
DisassociateDeviceFromRoom	Concede permissão para desassociar um dispositivo de sua sala atual	Write	device*		
DisassociateSkillFromSkillGroup	Concede permissão para desassociar uma skill de um grupo de skills	Write	skillgroup*		
DisassociateSkillFromUsers	Concede permissão para tornar uma skill privada indisponível para usuários inscritos e os impede de habilitá-la em seus respectivos dispositivos	Write	user*		
DisassociateSkillGroupFromRoom	Concede permissão para desassociar o grupo de skills de uma determinada sala	Write	room*		
			skillgroup*		
ForgetSmartHomeAppliances	Concede permissão para esquecer dispositivos domésticos inteligentes associados a uma sala	Write	room*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAddressBook	Concede permissão para obter os detalhes do catálogo de endereços pelo ARN do catálogo de endereços	Read	addressbook*		
GetConferencePreference	Concede permissão para recuperar as preferências de conferência existentes	Read			
GetConferenceProvider	Concede permissão para obter detalhes sobre um provedor de conferência específico	Read	conferenceprovider*		
GetContact	Concede permissão para obter os detalhes de contato pelo ARN do contato	Read	contact*		
GetDevice	Concede permissão para obter detalhes do dispositivo	Read	device*		
GetGateway	Concede permissão para recuperar os detalhes de um gateway	Read	gateway*		
GetGatewayGroup	Concede permissão para recuperar os detalhes de um grupo de gateways	Read	gatewaygroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetInvitationConfiguration	Concede permissão para recuperar os valores configurados para o modelo de e-mail de convite de inscrição de usuário	Read			
GetNetworkProfile	Concede permissão para obter os detalhes do perfil de rede pelo ARN do perfil de rede	Read	networkprofile*		
GetProfile	Concede permissão para obter um perfil quando provido de um ARN de perfil	Read	profile*		
GetRoom	Concede permissão para obter detalhes da sala	Read	room*		
GetRoomSkillParameter	Concede permissão para obter um parâmetro existente que foi definido para uma skill e uma sala	Read	room*		
GetSkillGroup	Concede permissão para obter detalhes do grupo de skills com o ARN do grupo de skills	Read	skillgroup*		
ListBusinessReportSchedules	Concede permissão para listar os detalhes das programações que um usuário configurou	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListConferenceProviders	Concede permissão para listar os provedores de conferências em um determinado Conta da AWS	Lista			
ListDeviceEvents	Concede permissão para listar o histórico de eventos do dispositivo, incluindo o status de conexão do dispositivo, por até 30 dias	List	device*		
ListGatewayGroups	Concede permissão para listar resumos de grupos de gateway	List			
ListGateways	Concede permissão para listar resumos de gateway	List	gatewaygroup*		
ListSkills	Concede permissão para listar skills	List			
ListSkillsStoreCategories	Concede permissão para listar todas as categorias na loja de skills da Alexa	List			
ListSkillsStoreSkillsByCategory	Concede permissão para listar todas as skills na loja de skills da Alexa por categoria	List			
ListSmartHomeAppliances	Concede permissão para listar todos os dispositivos domésticos inteligentes associados a uma sala	List	room*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTags	Concede permissão para listar todas as etiquetas de um recurso	Read	device		
			room		
			user		
PutConferencePreference	Concede permissão para definir as preferências da conferência em um provedor de conferência específico no nível da conta	Write			
PutDeviceSetupEvents [somente permissão]	Concede permissão para publicar eventos de configuração de dispositivo Alexa	Write			
PutInvitationConfiguration	Concede permissão para configurar o modelo de e-mail para o convite de inscrição de usuário com os atributos especificados	Write			
PutRoomSkillParameter	Concede permissão para colocar um parâmetro específico de sala para uma skill	Write	room*		
PutSkillAuthorization	Concede permissão para vincular a conta de um usuário a um provedor de skills terceirizado	Write	room*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RegisterAVSDevice	Concede permissão para registrar um dispositivo habilitado para a Alexa desenvolvido por um fabricante de equipamento original (OEM) usando o Alexa Voice Service (AVS)	Write		aws:RequestTag/${TagKey} aws:TagKeys	
RegisterDevice [somente permissão]	Concede permissão para registrar um dispositivo Alexa	Gravar			
RejectSkill	Concede permissão para desassociar uma habilidade da organização da de um usuário Conta da AWS	Gravar			
ResolveRoom	Concede permissão para resolver as informações da sala	Read			
RevokeInvitation	Concede permissão para revogar um convite	Write	user*		
SearchAddressBooks	Concede permissão para pesquisar catálogos de endereços e listar aqueles que atendem a um conjunto de critérios de filtragem e classificação	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SearchContacts	Concede permissão para pesquisar contatos e listar aqueles que atendem a um conjunto de critérios de filtragem e classificação	List			
SearchDevices	Concede permissão para pesquisar dispositivos	List			
SearchNetworkProfiles	Concede permissão para pesquisar perfis de rede e listar aqueles que atendem a um conjunto de critérios de filtragem e classificação	List			
SearchProfiles	Concede permissão para pesquisar perfis	List			
SearchRooms	Concede permissão para pesquisar salas	List			
SearchSkillGroups	Concede permissão para pesquisar grupos de skill	List			
SearchUsers	Concede permissão para pesquisar usuários	List			
SendAnnouncement	Concede permissão para acionar um fluxo assíncrono para enviar texto, SSML ou anúncios de áudio para salas identificadas por uma pesquisa ou filtro	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SendInvitation	Concede permissão para enviar um convite a um usuário	Write	user*		
StartDeviceSync	Concede permissão para restaurar o dispositivo e sua conta às configurações padrão conhecidas, apagando todas as informações e configurações definidas por seus usuários anteriores	Write			
StartSmartHomeApplianceDiscovery	Concede permissão para iniciar a descoberta de quaisquer dispositivos domésticos inteligentes associados à sala	Read	room*		
TagResource	Concede permissão para adicionar etiquetas de metadados a um recurso	Marcação	device		
			room		
			user		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover etiquetas de metadados de um recurso	Marcação	device		
			room		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			user		
UpdateAddressBook	Concede permissão para atualizar detalhes do catálogo de endereços pelo ARN do catálogo de endereços	Write	addressbook*		
UpdateBusinessReportSchedule	Concede permissão para atualizar a configuração da programação de entrega de relatórios com o ARN da programação especificada	Write	schedule*		
UpdateConferenceProvider	Concede permissão para atualizar as configurações de um provedor de conferência existente	Write	conferenceprovider*		
UpdateContact	Concede permissão para atualizar os detalhes de contato pelo ARN do contato	Write	contact*		
UpdateDevice	Concede permissão para atualizar o nome do dispositivo	Write	device*		
UpdateGateway	Concede permissão para atualizar os detalhes de um gateway	Write	gateway*		
UpdateGatewayGroup	Concede permissão para atualizar os detalhes de um grupo de gateways	Write	gatewaygroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateNetworkProfile	Concede permissão para atualizar um perfil de rede pelo ARN do perfil de rede	Write	networkprofile*		
UpdateProfile	Concede permissão para atualizar um perfil existente	Write	profile*		
UpdateRoom	Concede permissão para atualizar os detalhes da sala	Write	room*		
UpdateSkillGroup	Concede permissão para atualizar detalhes do grupo de skills com o ARN do grupo de skills	Write	skillgroup*		

Tipos de recursos definidos pelo Alexa for Business

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
profile	`arn:${Partition}:a4b:${Region}:${Account}:profile/${ResourceId}`	
room	`arn:${Partition}:a4b:${Region}:${Account}:room/${ResourceId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
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}	

Chaves de condição do Alexa for Business

O Alexa for Business define as seguintes chaves de condição que podem ser usadas no elemento `Condition`de uma política do IAM. É possível usar essas chaves para refinar ainda mais as

condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
a4b:amazonId	Filtra ações com base no ID da Amazon na solicitação	String
a4b:filters_deviceType	Filtra ações com base no tipo de dispositivo na solicitação	ArrayOfString
aws:RequestTag/${TagKey}	Filtra ações com base no conjunto de valores permitidos para cada uma das etiquetas	String
aws:ResourceTag/${TagKey}	Filtra ações com base no valor da etiqueta associada ao recurso	String
aws:TagKeys	Filtra ações com base na presença de etiquetas obrigatórias na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AmazonMediaImport

AmazonMediaImport (prefixo do serviço:`mediaimport`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AmazonMediaImport

- Tipos de recursos definidos pelo AmazonMediaImport
- Chaves de condição do AmazonMediaImport

Ações definidas pelo AmazonMediaImport

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDatabaseBinarySnapshot [somente permissão]	Concede permissão para criar um snapshot binário de banco de dados na conta AWS do cliente	Gravar			

Tipos de recursos definidos pelo AmazonMediaImport

AmazonMediaImport não suporta a especificação de um ARN de recurso no elemento de uma `Resource` declaração de política do IAM. Para conceder acesso ao AmazonMediaImport, especifique `"Resource": "*"` na política.

Chaves de condição do AmazonMediaImport

o mediaimport não tem chaves de contexto específicas do serviço que podem ser usadas no elemento `Condition` das instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Amplify

AWS Amplify (prefixo do serviço:`amplify`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.

- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Amplify
- Tipos de recursos definidos pelo AWS Amplify
- Chaves de condição do AWS Amplify

Ações definidas pelo AWS Amplify

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateWebACL	Concede permissão para associar uma WebACL a um recurso	Gravar	apps*		
CreateApp	Concede permissão para criar uma nova aplicação Amplify	Gravar	apps*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBackendEnvironment	Concede permissão para criar um novo ambiente de backend para uma aplicação Amplify	Gravar	apps*		
CreateBranch	Concede permissão para criar uma nova ramificação para uma aplicação Amplify	Gravar	branches*		
				aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
CreateDeployment	Concede permissão para criar uma implantação para aplicações de implantação manual. (Os aplicativos não estão conectados ao repositório)	Gravar	branches*		
CreateDomainAssociation	Concede permissão para criar um novo DomainAssociation em um aplicativo	Gravar	domains*		
CreateWebHook	Concede permissão para criar um novo webhook em uma aplicação	Gravar	branches*		
DeleteApp	Concede permissão para excluir uma aplicação do Amplify existente por appId	Gravar	apps*		
DeleteBackendEnvironment	Concede permissão para excluir uma ramificação para uma aplicação Amplify	Gravar	apps*		
DeleteBranch	Concede permissão para excluir uma ramificação para uma aplicação Amplify	Gravar	branches*		
DeleteDomainAssociation	Concede permissão para excluir um DomainAssociation	Gravar	domains*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteJob	Concede permissão para excluir um trabalho, para uma ramificação do Amplify, parte da aplicação Amplify	Gravar	jobs*		
DeleteWebHook	Concede permissão para excluir um webhook por ID	Gravar	webhooks*		
DisassociateWebACL	Concede permissão para desassociar uma WebACL de um recurso	Gravar	apps*		
GenerateAccessLogs	Concede permissão para gerar logs de acesso ao site para um intervalo de tempo específico por meio de um URL pré-assinado	Gravar	apps*		
GetApp	Concede permissão para recuperar uma aplicação do Amplify existente por appId	Leitura	apps*		
GetArtifactUrl	Concede permissão para recuperar informações de artefato correspondentes a um artifactId	Leitura	apps*		
GetBackendEnvironment	Concede permissão para recuperar um ambiente de backend para uma aplicação Amplify	Leitura	apps*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetBranch	Concede permissão para recuperar uma ramificação para uma aplicação Amplify	Leitura	branches*		
GetDomainAssociation	Concede permissão para recuperar informações de domínio correspondentes a um appId e domainName	Leitura	domains*		
GetJob	Concede permissão para obter um trabalho para uma ramificação, parte de uma aplicação Amplify	Leitura	jobs*		
GetWebACLForResource	Concede permissão para recuperar o WebACL associado a um recurso	Leitura	apps*		
GetWebHook	Concede permissão para recuperar as informações do webhook correspondentes a um webhookId	Leitura	webhooks*		
ListApps	Concede permissão para listar aplicações Amplify existentes	Lista			
ListArtifacts	Concede permissão para listar artefatos com uma aplicação, uma ramificação, um trabalho e um tipo de artefato	Lista	apps*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListBackendEnvironments	Concede permissão para listar ambientes de backend para uma aplicação Amplify	Lista	apps*		
ListBranches	Concede permissão para listar ramificações para uma aplicação Amplify	Lista	apps*		
ListDomainAssociations	Concede permissão para listar domínios com uma aplicação	Lista	apps*		
ListJobs	Concede permissão para listar trabalhos para uma ramificação, parte de uma aplicação Amplify	Lista	branches*		
ListResourcesForWebACL	Concede permissão para listar os recursos associados a uma WebACL	Lista			
ListTagsForResource	Concede permissão para listar tags para um recurso do AWS Amplify Console	Leitura	apps		
			branches		
			domains		
			webhooks		
ListWebHooks	Concede permissão para listar webhooks em uma aplicação	Lista	apps*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartDeployment	Concede permissão para iniciar uma implantação para aplicações de implantação manual. (Os aplicativos não estão conectados ao repositório)	Gravar	branches*		
StartJob	Concede permissão para iniciar um novo trabalho para uma ramificação, parte de uma aplicação	Gravar	jobs*		
StopJob	Concede permissão para interromper um trabalho que está em andamento, para uma ramificação do Amplify, parte da aplicação do Amplify	Gravar	jobs*		
TagResource	Concede permissão para marcar um recurso do AWS Amplify Console	Tags	apps		
			branches		
			domains		
			webhooks		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para remover uma tag de um recurso do AWS Amplify Console	Tags	apps		
			branches		
			domains		
			webhooks		
				aws:TagKeys	
UpdateApp	Concede permissão para atualizar uma aplicação Amplify existente	Gravar	apps*		
UpdateBranch	Concede permissão para atualizar uma ramificação para uma aplicação Amplify	Gravar	branches*		
UpdateDomainAssociation	Concede permissão para atualizar um DomainAssociation em um aplicativo	Gravar	domains*		
UpdateWebHook	Concede permissão para atualizar um webhook	Gravar	webhooks*		

Tipos de recursos definidos pelo AWS Amplify

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves

são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS Amplify

AWS O Amplify define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso pela chave e valor de uma etiqueta em uma solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pela chave da etiqueta associada ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta em uma solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS Amplify Admin

AWS O Amplify Admin (prefixo do serviço:`amplifybackend`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Amplify Admin
- Tipos de recursos definidos pelo AWS Amplify Admin
- Chaves de condição para o AWS Amplify Admin

Ações definidas pelo AWS Amplify Admin

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou

ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CloneBackend	Concede permissão para clonar um ambiente de backend do Amplify Admin existente em um novo ambiente de backend do Amplify Admin	Write	backend*		
CreateBackend	Concede permissão para criar um novo ambiente de backend do Amplify Admin pelo Amplify AppID	Gravar	created-backend*		
CreateBackendAPI	Concede permissão para criar uma API para um ambiente de back-end existente do Amplify Admin por AppID e backendEnvironmentName	Gravar	api*		
			backend*		
			environment*		
CreateBackendAuth	Concede permissão para criar um recurso de autenticação para um ambiente de back-end existente do Amplify Admin por AppID e backendEnvironmentName	Gravar	auth*		
			backend*		
			environment*		
CreateBackendConfig	Concede permissão para criar uma nova configuração de backend do Amplify Admin pelo ID do aplicativo Amplify	Gravar	config*		
CreateBackendStorage		Gravar	backend*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	Concede permissão para criar um recurso de armazenamento de backend		environment*		
			storage*		
CreateToken	Concede permissão para criar um token de desafio do Amplify Admin pelo ID do aplicativo	Gravar	backend*		
			token*		
DeleteBackend	Concede permissão para excluir um ambiente de back-end existente do Amplify Admin por AppID e backendEnvironmentName	Gravar	backend*		
			environment*		
DeleteBackendAPI	Concede permissão para excluir uma API de um ambiente de back-end existente do Amplify Admin por AppID e backendEnvironmentName	Gravar	api*		
			backend*		
			environment*		
DeleteBackendAuth	Concede permissão para excluir um recurso de autenticação de um ambiente de back-end existente do Amplify Admin por AppID e backendEnvironmentName	Gravar	auth*		
			backend*		
			environment*		
DeleteBackendStorage	Concede permissão para excluir um recurso de armazenamento de backend	Gravar	backend*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			environment*		
			storage*		
DeleteToken	Concede permissão para excluir um token de desafio do Amplify Admin pelo ID do aplicativo	Gravar	backend*		
			token*		
GenerateBackendAPIModels	Concede permissão para gerar modelos para uma API de um ambiente de back-end existente do Amplify Admin por AppID e backendEnvironmentName	Gravar	api*		
			backend*		
			environment*		
GetBackend	Concede permissão para recuperar um ambiente de back-end existente do Amplify Admin por AppID e backendEnvironmentName	Leitura	backend*		
			environment*		
GetBackendAPI	Concede permissão para recuperar uma API de um ambiente de back-end existente do Amplify Admin por AppID e backendEnvironmentName	Leitura	api*		
			backend*		
			environment*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetBackendAPIModels	Concede permissão para recuperar modelos para uma API de um ambiente de back-end existente do Amplify Admin por AppID e backendEnvironmentName	Leitura	api*		
			backend*		
			environment*		
GetBackendAuth	Concede permissão para recuperar um recurso de autenticação de um ambiente de back-end existente do Amplify Admin por AppID e backendEnvironmentName	Leitura	auth*		
			backend*		
			environment*		
GetBackendJob	Concede permissão para recuperar um trabalho de um ambiente de back-end existente do Amplify Admin por AppID e backendEnvironmentName	Leitura	backend*		
			job*		
GetBackendStorage	Concede permissão para recuperar um recurso de armazenamento de backend existente	Leitura	backend*		
			environment*		
GetToken	Concede permissão para recuperar um token de desafio do Amplify Admin pelo ID de aplicativo	Leitura	backend*		
			token*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ImportBackendAuth	Concede permissão para importar um recurso de autenticação existente de um ambiente de back-end do Amplify Admin por AppID e backendEnvironmentName	Gravar	auth*		
			backend*		
			environment*		
ImportBackendStorage	Concede permissão para importar um recurso de armazenamento de backend existente	Gravar	backend*		
			environment*		
			storage*		
ListBackendJobs	Concede permissão para recuperar as tarefas de um ambiente de back-end existente do Amplify Admin por AppID e backendEnvironmentName	Lista	backend*		
			job*		
ListS3Buckets	Concede permissão para recuperar buckets do s3	Lista			s3:ListAllMyBuckets
RemoveAllBackends	Concede permissão para excluir todos os ambientes de backend do Amplify Admin existentes pelo ID do aplicativo	Write	backend*		
			environment*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RemoveBackendConfig	Concede permissão para excluir uma configuração de backend do Amplify Admin pelo ID do aplicativo Amplify	Gravar	config*		
UpdateBackendAPI	Concede permissão para atualizar uma API de um ambiente de back-end existente do Amplify Admin por AppID e backendEnvironmentName	Gravar	api*		
			backend*		
			environment*		
UpdateBackendAuth	Concede permissão para atualizar um recurso de autenticação de um ambiente de back-end existente do Amplify Admin por AppID e backendEnvironmentName	Gravar	auth*		
			backend*		
			environment*		
UpdateBackendConfig	Concede permissão para atualizar uma configuração de backend do Amplify Admin pelo ID do aplicativo Amplify	Gravar	config*		
UpdateBackendJob	Concede permissão para atualizar um trabalho de um ambiente de back-end existente do Amplify Admin por AppID e backendEnvironmentName	Gravar	backend*		
			job*		
UpdateBackendStorage		Gravar	backend*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	Concede permissão para atualizar um recurso de armazenamento de backend		environment*		
			storage*		

Tipos de recursos definidos pelo AWS Amplify Admin

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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/*`	

Tipos de recursos	ARN	Chaves de condição
auth	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/auth/*`	
job	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/job/*`	
config	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/config/*`	
token	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/challenge/*`	
storage	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/storage/*`	

Chaves de condição para o AWS Amplify Admin

Amplify Admin não tem chaves de contexto específicas de serviço que podem ser usadas no `Condition` elemento de instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Amplify UI Builder

AWS O Amplify UI Builder (prefixo do serviço:`amplifyuibuilder`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.

- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Amplify UI Builder
- Tipos de recursos definidos pelo AWS Amplify UI Builder
- Chaves de condição do AWS Amplify UI Builder

Ações definidas pelo AWS Amplify UI Builder

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateComponent	Concede permissão para criar um componente	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	amplify:GetApp amplifyuibuilder:GetComponent amplifyuibuilder:TagResource
CreateForm	Concede permissão para criar um formulário	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	amplify:GetApp amplifyuibuilder:GetForm amplifyuibuilder:T

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					agResource amplifyuibuilder:UntagResource
CreateTheme	Concede permissão para criar um tema	Write		aws:RequestTag/${TagKey} aws:TagKeys	amplify:GetApp amplifyuibuilder:GetTheme amplifyuibuilder:TagResource
DeleteComponent	Concede permissão para excluir um componente	Gravar	ComponentResource*		amplify:GetApp amplifyuibuilder:UntagResource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteForm	Concede permissão para excluir um formulário	Gravar	FormResource*		amplify:GetApp amplifyuibuilder:TagResource amplifyuibuilder:UntagResource
DeleteTheme	Concede permissão para excluir um tema	Write	ThemeResource*		amplify:GetApp amplifyuibuilder:UntagResource
ExchangeCodeForToken	Concede permissão para trocar um código por um token	Write			
ExportComponents	Concede permissão para exportar componentes	Leitura			
ExportForms	Concede permissão para exportar formulários	Leitura			
ExportThemes	Concede permissão para exportar temas	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetCodegenJob	Concede permissão para obter um trabalho de codegen existente	Leitura	CodegenJobResource*		amplify:GetApp
GetComponent	Concede permissão para obter um componente existente	Leitura	ComponentResource*		amplify:GetApp
GetForm	Concede permissão para obter um formulário existente	Leitura	FormResource*		amplify:GetApp
GetMetadata	Concede permissão para obter um metadado existente	Leitura			
GetTheme	Concede permissão para obter um tema existente	Leitura	ThemeResource*		amplify:GetApp
ListCodegenJobs	Concede permissão para listar trabalhos de codegen	Lista			amplify:GetApp
ListComponents	Concede permissão para listar componentes	Lista			amplify:GetApp
ListForms	Concede permissão para listar formulários	Lista			amplify:GetApp
ListTagsForResource	Concede permissão para listar tags de um nome do recurso da Amazon (ARN) especificado	Lista	CodegenJobResource		
			ComponentResource		
			FormResource		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			ThemeResource		
ListThemes	Concede permissão para listar temas	Lista			amplify:GetApp
PutMetadataFlag	Concede permissão para colocar um metadado existente	Gravar			
RefreshToken	Concede permissão para atualizar um token de acesso	Gravar			
ResetMetadataFlag	Concede permissão para redefinir um metadado existente	Gravar			
StartCodegenJob	Concede permissão para iniciar um trabalho de codegen	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	amplify:GetApp
TagResource	Concede permissão para marcar o recurso com uma chave e um valor de tags	Tags	CodegenJobResource		
			ComponentResource		
			FormResource		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			ThemeResource		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para desmarcar um recurso com um nome do recurso da Amazon (ARN) especificado	Tags	CodegenJobResource		
			ComponentResource		
			FormResource		
			ThemeResource		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateComponent	Concede permissão para atualizar um componente	Gravar	ComponentResource*		amplify:GetApp amplifyuibuilder:TagResource amplifyuibuilder:UntagResource
UpdateForm	Concede permissão para atualizar um formulário	Gravar	FormResource*		amplify:GetApp amplifyuibuilder:GetForm amplifyuibuilder:TagResource amplifyuibuilder:UntagResource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateTheme	Concede permissão para atualizar um tema	Write	ThemeResource*		amplify:GetApp amplifyuibuilder:GetTheme amplifyuibuilder:TagResource amplifyuibuilder:UntagResource

Tipos de recursos definidos pelo AWS Amplify UI Builder

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
CodegenJobResource	`arn:${Partition}:amplifyuibuilder:${Region}:${Account}:app/${AppId}/envi`	amplifyuibuilder:CodegenJobResourceAppId

Tipos de recursos	ARN	Chaves de condição
	ronment/${EnvironmentName}/codegen-jobs/${Id}	amplifyuibuilder:CodegenJobResourceEnvironmentName amplifyuibuilder:CodegenJobResourceId aws:ResourceTag/${TagKey}
Component Resource	arn:${Partition}:amplifyuibuilder:${Region}:${Account}:app/${AppId}/environment/${EnvironmentName}/components/${Id}	amplifyuibuilder:ComponentResourceAppId amplifyuibuilder:ComponentResourceEnvironmentName amplifyuibuilder:ComponentResourceId aws:ResourceTag/${TagKey}
FormResource	arn:${Partition}:amplifyuibuilder:${Region}:${Account}:app/${AppId}/environment/${EnvironmentName}/forms/${Id}	amplifyuibuilder:FormResourceAppId amplifyuibuilder:FormResourceEnvironmentName amplifyuibuilder:FormResourceId aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
ThemeResource	`arn:${Partition}:amplifyuibuilder:${Region}:${Account}:app/${AppId}/environment/${EnvironmentName}/themes/${Id}`	amplifyuibuilder:ThemeResourceAppId amplifyuibuilder:ThemeResourceEnvironmentName amplifyuibuilder:ThemeResourceId aws:ResourceTag/${TagKey}

Chaves de condição do AWS Amplify UI Builder

AWS O Amplify UI Builder define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
amplifyuibuilder:CodegenJobResourceAppId	Filtra o acesso pelo ID da aplicação	String
amplifyuibuilder:CodegenJob	Filtra o acesso pelo nome de ambiente do backend	String

Chaves de condição	Descrição	Tipo
ResourceEnvironmentName		
amplifyuibuilder:CodegenJobResourceId	Filtra o acesso pelo ID do trabalho de codegen	String
amplifyuibuilder:ComponentResourceAppId	Filtra o acesso pelo ID da aplicação	String
amplifyuibuilder:ComponentResourceEnvironmentName	Filtra o acesso pelo nome de ambiente do backend	String
amplifyuibuilder:ComponentResourceId	Filtra o acesso pelo ID do componente	String
amplifyuibuilder:FormResourceAppId	Filtra o acesso pelo ID da aplicação	String
amplifyuibuilder:FormResourceEnvironmentName	Filtra o acesso pelo nome de ambiente do backend	String

Chaves de condição	Descrição	Tipo
amplifyuibuilder:FormResourceId	Filtra o acesso pelo ID do formulário	String
amplifyuibuilder:ThemeResourceAppId	Filtra o acesso pelo ID da aplicação	String
amplifyuibuilder:ThemeResourceEnvironmentName	Filtra o acesso pelo nome de ambiente do backend	String
amplifyuibuilder:ThemeResourceId	Filtra o acesso pelo ID do tema	String
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Apache Kafka para clusters APIs Amazon MSK

O Apache Kafka para clusters do APIs Amazon MSK (prefixo do serviço:`kafka-cluster`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Apache Kafka para clusters APIs Amazon MSK
- Tipos de recursos definidos pelo Apache Kafka para clusters APIs Amazon MSK
- Chaves de condição do Apache Kafka para clusters do APIs Amazon MSK

Ações definidas pelo Apache Kafka para clusters APIs Amazon MSK

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa

ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AlterCluster	Concede permissão para alterar vários aspectos do cluster, equivalente a ALTER CLUSTER ACL do Apache Kafka.	Write	cluster*		kafka-cluster:Connect kafka-cluster:DescribeCluster

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AlterClusterDynamicConfiguration	Concede permissão para alterar a configuração dinâmica de um cluster, equivalente a ALTER_CONFIGS CLUSTER ACL do Apache Kafka.	Write	cluster*		kafka-cluster:Connect kafka-cluster:DescribeClusterDynamicConfiguration
AlterGroup	Concede permissão para entrar em grupos de um cluster, equivalente a READ GROUP ACL do Apache Kafka.	Write	group*		kafka-cluster:Connect kafka-cluster:DescribeGroup
AlterTopic	Concede permissão para alterar os tópicos de um cluster, equivalente a ALTER TOPIC ACL do Apache Kafka.	Write	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopic

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AlterTopicDynamicConfiguration	Concede permissão para alterar a configuração dinâmica dos tópicos de um cluster, equivalente a ALTER_CONFIGS TOPIC ACL do Apache Kafka.	Gravar	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopicDynamicConfiguration
AlterTransactionalId	Concede permissão para alterar a transação IDs em um cluster, equivalente à ACL WRITE TRANSACTIONAL_ID do Apache Kafka	Gravar	transactional-id*		kafka-cluster:Connect kafka-cluster:DescribeTransactionalId kafka-cluster:WriteData
Connect	Concede permissão para se conectar e se autenticar no cluster.	Gravar	cluster*		
CreateTopic	Concede permissão para criar tópicos em um cluster, equivalente à CREATE ACL do Apache Kafka CLUSTER/TOPIC	Gravar	topic*		kafka-cluster:Connect

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteGroup	Concede permissão para excluir grupos de um cluster, equivalente a DELETE GROUP ACL do Apache Kafka.	Write	group*		kafka-cluster:Connect kafka-cluster:DescribeGroup
DeleteTopic	Concede permissão para excluir tópicos de um cluster, equivalente a DELETE TOPIC ACL do Apache Kafka.	Write	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopic
DescribeCluster	Concede permissão para descrever vários aspectos do cluster, equivalente a DESCRIBE CLUSTER ACL do Apache Kafka.	List	cluster*		kafka-cluster:Connect
DescribeClusterDynamicConfiguration	Concede permissão para descrever a configuração dinâmica de um cluster, equivalente a DESCRIBE_ CONFIGS CLUSTER ACL do Apache Kafka.	List	cluster*		kafka-cluster:Connect

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeGroup	Concede permissão para descrever os grupos de um cluster, equivalente a DESCRIBE GROUP ACL do Apache Kafka.	List	group*		kafka-cluster:Connect
DescribeTopic	Concede permissão para descrever os tópicos de um cluster, equivalente a DESCRIBE TOPIC ACL do Apache Kafka.	List	topic*		kafka-cluster:Connect
DescribeTopicDynamicConfiguration	Concede permissão para descrever a configuração dinâmica dos tópicos de um cluster, equivalente a DESCRIBE_CONFIGS TOPIC ACL do Apache Kafka.	Lista	topic*		kafka-cluster:Connect
DescribeTransactionalId	Concede permissão para descrever transações IDs em um cluster, equivalente à ACL DESCRIBE TRANSACTIONAL_ID do Apache Kafka	Lista	transactional-id*		kafka-cluster:Connect

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ReadData	Concede permissão para ler dados dos tópicos de um cluster, equivalente a READ TOPIC ACL do Apache Kafka.	Read	topic*		kafka-cluster:AlterGroup kafka-cluster:Connect kafka-cluster:DescribeTopic
WriteData	Concede permissão para gravar dados em tópicos de um cluster, equivalente a WRITE TOPIC ACL do Apache Kafka.	Write	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopic
WriteData Idempotently	Concede permissão para gravar dados em um cluster de modo idempotente, equivalente a IDEMPOTENT_WRITE CLUSTER ACL do Apache Kafka.	Gravar	cluster*		kafka-cluster:Connect kafka-cluster:WriteData

Tipos de recursos definidos pelo Apache Kafka para clusters APIs Amazon MSK

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso

também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}`	

Chaves de condição do Apache Kafka para clusters do APIs Amazon MSK

O Apache Kafka para clusters do APIs Amazon MSK define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:ResourceTag/${TagKey}	Filtra ações com base nos pares de chave-valor da etiqueta anexados ao recurso A chave de contexto da tag de recurso só se aplicará ao recurso do cluster, não a tópicos, grupos e transações IDs	String

Ações, recursos e chaves de condição do Amazon API Gateway

O Amazon API Gateway (prefixo do serviço: `execute-api`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon API Gateway
- Tipos de recursos definidos pelo Amazon API Gateway
- Chaves de condição do Amazon API Gateway

Ações definidas pelo Amazon API Gateway

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o

nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
InvalidateCache	Usado para invalidar o cache da API quando da solicitação de um cliente	Write	execute-api-general*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
Invoke	Usado para invocar uma API quando de uma solicitação de cliente	Gravar	execute-api-domain		
			execute-api-general		
ManageConnections	ManageConnections controla o acesso à API @connections	Gravar	execute-api-general*		

Tipos de recursos definidos pelo Amazon API Gateway

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
execute-api-general	`arn:${Partition}:execute-api:${Region}:${Account}:${ApiId}/${Stage}/${Method}/${ApiSpecificResourcePath}`	execute-api:viaDomainArn
execute-api-domain	`arn:${Partition}:execute-api:${Region}:${Account}:/domainnames/${DomainName} ${DomainIdentifier}`	

Chaves de condição do Amazon API Gateway

O Amazon API Gateway define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
execute-api:viaDomainArn	Filtra o acesso pelo nome de domínio ARN do qual a API é chamada	String

Ações, recursos e chaves de condição do AWS App Mesh

AWS O App Mesh (prefixo do serviço:`appmesh`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS App Mesh
- Tipos de recursos definidos pelo AWS App Mesh
- Chaves de condição do AWS App Mesh

Ações definidas pelo AWS App Mesh

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando

usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateGatewayRoute	Concede permissão para criar uma rota de gateway associada a um gateway virtual	Write	gatewayRoute*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualService		
CreateMesh	Concede permissão para criar uma malha de serviço	Write	mesh*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateRoute	Concede permissão para criar uma rota associada a um roteador virtual	Write	route*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualNode		
CreateVirtualGateway	Concede permissão para criar um gateway virtual dentro de uma malha de serviço	Write	virtualGateway*		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey}	
CreateVirtualNode	Concede permissão para criar um nó virtual dentro de uma malha de serviço	Write	virtualNode*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualService		
CreateVirtualRouter	Concede permissão para criar um roteador virtual dentro de uma malha de serviço	Write	virtualRouter*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateVirtualService	Concede permissão para criar um serviço virtual dentro de uma malha de serviço	Write	virtualService*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualNode		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			virtualRouter		
DeleteGatewayRoute	Concede permissão para excluir uma rota de gateway existente	Write	gatewayRoute*		
DeleteMesh	Concede permissão para excluir uma malha de serviço existente	Gravar	mesh*		
DeleteMeshPolicy [somente permissão]	Concede permissão para excluir a política de controle de acesso ao RAM de uma malha	Gravar	mesh*		
DeleteRoute	Concede permissão para excluir uma rota existente	Write	route*		
DeleteVirtualGateway	Concede permissão para excluir um gateway virtual existente	Write	virtualGateway*		
DeleteVirtualNode	Concede permissão para excluir um nó virtual existente	Write	virtualNode*		
DeleteVirtualRouter	Concede permissão para excluir um roteador virtual existente	Write	virtualRouter*		
DeleteVirtualService	Concede permissão para excluir um serviço virtual existente	Write	virtualService*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeGatewayRoute	Concede permissão para descrever uma rota de gateway existente	Read	gatewayRoute*		
DescribeMesh	Concede permissão para descrever uma malha de serviço existente	Read	mesh*		
DescribeRoute	Concede permissão para descrever uma rota existente	Read	route*		
DescribeVirtualGateway	Concede permissão para descrever um gateway virtual existente	Read	virtualGateway*		
DescribeVirtualNode	Concede permissão para descrever um nó virtual existente	Read	virtualNode*		
DescribeVirtualRouter	Concede permissão para descrever um roteador virtual existente	Read	virtualRouter*		
DescribeVirtualService	Concede permissão para descrever um serviço virtual existente	Leitura	virtualService*		
GetMeshPolicy [somente permissão]	Concede permissão para ler a política de controle de acesso ao RAM para uma malha	Leitura	mesh*		
ListGatewayRoutes	Concede permissão para listar rotas de gateway existentes em uma malha de serviço	List	virtualGateway*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListMeshes	Concede permissão para listar malhas de serviço existentes	List			
ListRoutes	Concede permissão para listar rotas existentes em uma malha de serviço	List	virtualRouter*		
ListTagsForResource	Concede permissão para listar as etiquetas para um recurso do App Mesh	List	gatewayRoute		
			mesh		
			route		
			virtualGateway		
			virtualNode		
			virtualRouter		
			virtualService		
ListVirtualGateways	Concede permissão para listar gateways virtuais existentes em uma malha de serviço	List	mesh*		
ListVirtualNodes	Concede permissão para listar nós virtuais existentes	List	mesh*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListVirtualRouters	Concede permissão para listar roteadores virtuais existentes em uma malha de serviço	List	mesh*		
ListVirtualServices	Concede permissão para listar serviços virtuais existentes em uma malha de serviço	Lista	mesh*		
PutMeshPolicy [somente permissão]	Concede permissão para definir a política de controle de acesso ao RAM para uma malha	Gravar	mesh*		
StreamAggregatedResources	Concede permissão para receber recursos transmitidos para um endpoint do App Mesh (/) VirtualNode VirtualGateway	Leitura	virtualGateway		
			virtualNode		
TagResource	Concede permissão para etiquetar um recurso com um resourceArn especificado	Tags	gatewayRoute		
			mesh		
			route		
			virtualGateway		
			virtualNode		
			virtualRouter		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			virtualService		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para excluir uma etiqueta de um recurso	Tags	gatewayRoute		
			mesh		
			route		
			virtualGateway		
			virtualNode		
			virtualRouter		
			virtualService		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateGatewayRoute	Concede permissão para atualizar uma rota de gateway existente para uma malha de serviço especificada e um gateway virtual	Write	gatewayRoute*		
			virtualService		
UpdateMesh	Concede permissão para atualizar uma malha de serviço existente	Write	mesh*		
UpdateRoute	Concede permissão para atualizar uma rota existente para uma malha de serviço especificada e um roteador virtual	Write	route*		
			virtualNode		
UpdateVirtualGateway	Concede permissão para atualizar um gateway virtual existente em uma malha de serviço especificada	Write	virtualGateway*		
UpdateVirtualNode	Concede permissão para atualizar um nó virtual existente em uma malha de serviço especificada	Write	virtualNode*		
UpdateVirtualRouter	Concede permissão para atualizar um roteador virtual existente em uma malha de serviço especificada	Write	virtualRouter*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateVirtualService	Concede permissão para atualizar um serviço virtual existente em uma malha de serviço especificada	Write	virtualService*		
			virtualNode		
			virtualRouter		

Tipos de recursos definidos pelo AWS App Mesh

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
mesh	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}`	aws:ResourceTag/${TagKey}
virtualService	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualService/${VirtualServiceName}`	aws:ResourceTag/${TagKey}
virtualNode	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualNode/${VirtualNodeName}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS App Mesh

AWS O App Mesh define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações pela presença de pares de chave-valor da etiqueta na solicitação.	String

Chaves de condição	Descrição	Type
aws:ResourceTag/${TagKey}	Filtra as ações pelos pares de valor-chave da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição da pré-visualização do AWS App Mesh

AWS O App Mesh Preview (prefixo do serviço:`appmesh-preview`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela pré-visualização do AWS App Mesh
- Tipos de recursos definidos pela pré-visualização do AWS App Mesh
- Chaves de condição da Visualização do AWS App Mesh

Ações definidas pela pré-visualização do AWS App Mesh

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateGatewayRoute	Concede permissão para criar uma rota de gateway associada a um gateway virtual	Write	gatewayRoute*		
			virtualService		
CreateMesh	Concede permissão para criar uma malha de serviço	Write	mesh*		
CreateRoute	Concede permissão para criar uma rota associada a um roteador virtual	Write	route*		
			virtualNode		
CreateVirtualGateway	Concede permissão para criar um gateway virtual dentro de uma malha de serviço	Write	virtualGateway*		
CreateVirtualNode	Concede permissão para criar um nó virtual dentro de uma malha de serviço	Write	virtualNode*		
			virtualService		
CreateVirtualRouter	Concede permissão para criar um roteador virtual dentro de uma malha de serviço	Write	virtualRouter*		
CreateVirtualService	Concede permissão para criar um serviço virtual dentro de uma malha de serviço	Write	virtualService*		
			virtualNode		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			virtualRouter		
DeleteGatewayRoute	Concede permissão para excluir uma rota de gateway existente	Write	gatewayRoute*		
DeleteMesh	Concede permissão para excluir uma malha de serviço existente	Gravar	mesh*		
DeleteMeshPolicy [somente permissão]	Concede permissão para excluir a política de controle de acesso ao RAM de uma malha	Gravar	mesh*		
DeleteRoute	Concede permissão para excluir uma rota existente	Write	route*		
DeleteVirtualGateway	Concede permissão para excluir um gateway virtual existente	Write	virtualGateway*		
DeleteVirtualNode	Concede permissão para excluir um nó virtual existente	Write	virtualNode*		
DeleteVirtualRouter	Concede permissão para excluir um roteador virtual existente	Write	virtualRouter*		
DeleteVirtualService	Concede permissão para excluir um serviço virtual existente	Write	virtualService*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeGatewayRoute	Concede permissão para descrever uma rota de gateway existente	Read	gatewayRoute*		
DescribeMesh	Concede permissão para descrever uma malha de serviço existente	Read	mesh*		
DescribeRoute	Concede permissão para descrever uma rota existente	Read	route*		
DescribeVirtualGateway	Concede permissão para descrever um gateway virtual existente	Read	virtualGateway*		
DescribeVirtualNode	Concede permissão para descrever um nó virtual existente	Read	virtualNode*		
DescribeVirtualRouter	Concede permissão para descrever um roteador virtual existente	Read	virtualRouter*		
DescribeVirtualService	Concede permissão para descrever um serviço virtual existente	Leitura	virtualService*		
GetMeshPolicy [somente permissão]	Concede permissão para ler a política de controle de acesso ao RAM para uma malha	Leitura	mesh*		
ListGatewayRoutes	Concede permissão para listar rotas de gateway existentes em uma malha de serviço	List	virtualGateway*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListMeshes	Concede permissão para listar malhas de serviço existentes	List			
ListRoutes	Concede permissão para listar rotas existentes em uma malha de serviço	List	virtualRouter*		
ListVirtualGateways	Concede permissão para listar gateways virtuais existentes em uma malha de serviço	List	mesh*		
ListVirtualNodes	Concede permissão para listar nós virtuais existentes	List	mesh*		
ListVirtualRouters	Concede permissão para listar roteadores virtuais existentes em uma malha de serviço	List	mesh*		
ListVirtualServices	Concede permissão para listar serviços virtuais existentes em uma malha de serviço	Lista	mesh*		
PutMeshPolicy [somente permissão]	Concede permissão para definir a política de controle de acesso ao RAM para uma malha	Gravar	mesh*		
StreamAggregatedResources	Concede permissão para receber recursos transmitidos para um endpoint do App Mesh (/) VirtualNode VirtualGateway	Leitura	virtualGateway		
			virtualNode		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateGatewayRoute	Concede permissão para atualizar uma rota de gateway existente para uma malha de serviço especificada e um gateway virtual	Write	gatewayRoute*		
			virtualService		
UpdateMesh	Concede permissão para atualizar uma malha de serviço existente	Write	mesh*		
UpdateRoute	Concede permissão para atualizar uma rota existente para uma malha de serviço especificada e um roteador virtual	Write	route*		
			virtualNode		
UpdateVirtualGateway	Concede permissão para atualizar um gateway virtual existente em uma malha de serviço especificada	Write	virtualGateway*		
UpdateVirtualNode	Concede permissão para atualizar um nó virtual existente em uma malha de serviço especificada	Write	virtualNode*		
UpdateVirtualRouter	Concede permissão para atualizar um roteador virtual existente em uma malha de serviço especificada	Write	virtualRouter*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateVirtualService	Concede permissão para atualizar um serviço virtual existente em uma malha de serviço especificada	Write	virtualService*		
			virtualNode		
			virtualRouter		

Tipos de recursos definidos pela pré-visualização do AWS App Mesh

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
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}`	

Chaves de condição da Visualização do AWS App Mesh

A Visualização do App Mesh não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS App Runner

AWS O App Runner (prefixo do serviço:`apprunner`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS App Runner
- Tipos de recurso definidos pelo AWS App Runner
- Chaves de condição do AWS App Runner

Ações definidas pelo AWS App Runner

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateCustomDomain	Concede permissão para associar seu próprio nome de domínio ao URL do subdomínio AWS App Runner do seu serviço App Runner	Gravar	service*		
AssociateWebAcl [somente permissão]	Concede permissão para associar o serviço a uma Web ACL AWS do WAF	Gravar	service* webacl*		
CreateAutoScalingConfiguration	Concede permissão para criar um recurso de configuração de escalonamento automático do AWS App Runner	Gravar	autoscalingconfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateConnection	Concede permissão para criar um recurso de conexão AWS do App Runner	Gravar	connection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateObservabilityConfiguration	Concede permissão para criar um recurso de configuração de observabilidade do AWS App Runner	Gravar	observabilityconfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateService	Concede permissão para criar um recurso de serviço AWS do App Runner	Gravar	service*		
			autoscalingconfiguration		
			connection		
			observabilityconfiguration		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			vpcconnector		
				aws:RequestTag/${TagKey} aws:TagKeys apprunner:ConnectionArn apprunner:AutoScalingConfigurationArn apprunner:ObservabilityConfigurationArn apprunner:VpcConnectorArn	
CreateVpcConnector	Concede permissão para criar um recurso de AWS conector VPC do App Runner	Gravar	vpcconnector*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVpcIngressConnection	Concede permissão para criar um recurso AWS do App Runner VpcIngressConnection	Gravar	vpcingressconnection*		
				aws:RequestTag/${TagKey} aws:TagKeys apprunner:ServiceArn apprunner:VpcId apprunner:VpcEndpointId	
DeleteAutoScalingConfiguration	Concede permissão para excluir um recurso de configuração de escalonamento automático do AWS App Runner	Gravar	autoscalingconfiguration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteConnection	Concede permissão para excluir um recurso de conexão AWS do App Runner	Gravar	connection*		
DeleteObservabilityConfiguration	Concede permissão para excluir um recurso de configuração de observabilidade do AWS App Runner	Gravar	observabilityconfiguration*		
DeleteService	Concede permissão para excluir um recurso de serviço AWS do App Runner	Gravar	service*		
DeleteVpcConnector	Concede permissão para excluir um recurso de AWS conector VPC do App Runner	Gravar	vpcconnector*		
DeleteVpcIngressConnection	Concede permissão para excluir um recurso AWS do App Runner VpcIngressConnection	Gravar	vpcingressconnection*		
DescribeAutoScalingConfiguration	Concede permissão para recuperar a descrição de um recurso de configuração de escalonamento automático do AWS App Runner	Leitura	autoscalingconfiguration*		
DescribeCustomDomains	Concede permissão para recuperar descrições de nomes de domínio personalizados associados a um serviço AWS App Runner	Leitura	service*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeObservabilityConfiguration	Concede permissão para recuperar a descrição de um recurso de configuração de observabilidade do AWS App Runner	Leitura	observabilityconfiguration*		
DescribeOperation	Concede permissão para recuperar a descrição de uma operação que ocorreu em um serviço AWS App Runner	Leitura	service*		
DescribeService	Concede permissão para recuperar a descrição de um recurso de serviço do AWS App Runner	Leitura	service*		
DescribeVpcConnector	Concede permissão para recuperar a descrição de um recurso de conector VPC do AWS App Runner	Leitura	vpcconnector*		
DescribeVpcIngressConnection	Concede permissão para recuperar a descrição de um recurso do AWS App Runner VpcIngressConnection	Leitura	vpcingressconnection*		
DescribeWebAclForService [somente permissão]	Concede permissão para obter a Web ACL do AWS WAF associada a um serviço AWS App Runner	Leitura	service*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateCustomDomain	Concede permissão para desassociar um nome de domínio personalizado de um serviço do AWS App Runner	Gravar	service*		
DisassociateWebAcl [somente permissão]	Concede permissão para desassociar o serviço com uma Web ACL do AWS WAF	Gravar	service*		
ListAssociatedServicesForWebAcl [somente permissão]	Concede permissão para listar os serviços associados a uma Web ACL AWS do WAF	Lista	webacl*		
ListAutoScalingConfigurations	Concede permissão para recuperar uma lista de configurações de escalonamento automático do AWS App Runner em seu Conta da AWS	Lista			
ListConnections	Concede permissão para recuperar uma lista de conexões do AWS App Runner em seu Conta da AWS	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListObservabilityConfigurations	Concede permissão para recuperar uma lista de configurações de observabilidade do AWS App Runner em seu Conta da AWS	Lista			
ListOperations	Concede permissão para recuperar uma lista de operações que ocorreram em um recurso de serviço do AWS App Runner	Lista	service*		
ListServices	Concede permissão para recuperar uma lista dos serviços do AWS App Runner em execução no seu Conta da AWS	Lista			
ListServicesForAutoScalingConfiguration	Concede permissão para recuperar uma lista de AppRunner serviços associados de uma configuração de escalabilidade automática do AWS App Runner em seu Conta da AWS	Lista	autoscalingconfiguration*		
ListTagsForResource	Concede permissão para listar tags associadas a um recurso AWS do App Runner	Leitura	autoscalingconfiguration		
			connection		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			observabilityconfiguration		
			service		
			vpcconnector		
ListVpcConnectors	Concede permissão para recuperar uma lista de conectores VPC do AWS App Runner em seu Conta da AWS	Lista			
ListVpcIngressConnections	Concede permissão para recuperar uma lista do AWS App Runner VpcIngressConnections em seu Conta da AWS	Lista			
PauseService	Concede permissão para pausar um serviço ativo do AWS App Runner	Gravar	service*		
ResumeService	Concede permissão para retomar um serviço ativo AWS do App Runner	Gravar	service*		
StartDeployment	Concede permissão para iniciar uma implantação manual em um serviço App Runner AWS	Gravar	service*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para adicionar tags ou atualizar valores de tag de um recurso do AWS App Runner	Tags	autoscalingconfiguration		
			connection		
			observabilityconfiguration		
			service		
			vpcconnector		
			vpcingressconnection		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover tags de um recurso do AWS App Runner	Tags	autoscalingconfiguration		
			connection		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			observabilityconfiguration		
			service		
			vpcconnector		
			vpcingressconnection		
				aws:TagKeys	
UpdateDefaultAutoScalingConfiguration	Concede permissão para atualizar uma configuração de escalonamento automático do AWS App Runner para ser a padrão em seu Conta da AWS	Gravar	autoscalingconfiguration*		
UpdateService	Concede permissão para atualizar um recurso de serviço AWS do App Runner	Gravar	service*		
			autoscalingconfiguration		
			connection		
			observabilityconfiguration		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			vpcconnector		
				apprunner:ConnectionArn apprunner:AutoScalingConfigurationArn apprunner:ObservabilityConfigurationArn apprunner:VpcConnectorArn	
UpdateVpcIngressConnection	Concede permissão para atualizar um recurso AWS do App Runner VpcIngressConnection	Gravar	vpcingressconnection*		
				apprunner:VpcId apprunner:VpcEndpointId	

Tipos de recurso definidos pelo AWS App Runner

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
vpcingressconnection	`arn:${Partition}:apprunner:${Region}:${Account}:vpcingressconnection/${VpcIngressConnectionName}/${VpcIngressConnectionId}`	aws:ResourceTag/${TagKey}
webacl	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/webacl/${Name}/${Id}`	

Chaves de condição do AWS App Runner

AWS O App Runner define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
apprunner:AutoScalingConfigurationArn	Filtra o acesso pelas UpdateService ações CreateService e com base no ARN de um recurso associado AutoScalingConfiguration	ARN
apprunner:ConnectionArn	Filtra o acesso pelas UpdateService ações CreateService e com base no ARN de um recurso de conexão associado	ARN
apprunner:Observab	Filtra o acesso pelas UpdateService ações CreateService e com base no ARN de um recurso associado ObservabilityConfiguration	ARN

Chaves de condição	Descrição	Tipo
ilityConfiguration Arn		
apprunner :ServiceArn	Filtra o acesso pela CreateVpcIngressConnection ação com base no ARN de um recurso de serviço associado	ARN
apprunner :VpcConne ctorArn	Filtra o acesso pelas UpdateService ações CreateSer vice e com base no ARN de um recurso associado VpcConnector	ARN
apprunner :VpcEndpointId	Filtra o acesso pelas UpdateVpcIngressConnection ações CreateVpcIngressConnection e com base no VPC Endpoint na solicitação	String
apprunner:VpcId	Filtra o acesso pelas UpdateVpcIngressConnection ações CreateVpcIngressConnection e com base na VPC na solicitação	String
aws:Reque stTag/${TagKey}	Filtra o acesso por ações com base na presença de pares de chave-valor da etiqueta na solicitação	String
aws:Resou rceTag/${ TagKey}	Filtra o acesso por ações com base nos pares de chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso por ações com base na presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS App Studio

AWS O App Studio (prefixo do serviço:`appstudio`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.

- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS App Studio
- Tipos de recursos definidos pelo AWS App Studio
- Chaves de condição do AWS App Studio

Ações definidas pelo AWS App Studio

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAccountStatus [somente permissão]	Concede permissão para descrever o status atual da conta	Leitura			
GetEnablementJobStatus [somente permissão]	Concede permissão para buscar o status de um trabalho de capacitação	Leitura			
StartEnablementJob [somente permissão]	Concede permissão para enviar um trabalho de capacitação	Gravar			
StartRollbackEnablementJob [somente permissão]	Concede permissão para reverter um trabalho de capacitação	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartTeamDeployment [somente permissão]	Concede permissão para iniciar uma implantação de equipe	Gravar			

Tipos de recursos definidos pelo AWS App Studio

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
instance	`arn:${Partition}:appstudio:${Region}:${Account}:instance/${InstanceId}`	
application	`arn:${Partition}:appstudio:${Region}:${Account}:application/${ApplicationId}`	
connector	`arn:${Partition}:appstudio:${Region}:${Account}:connector/${ConnectionId}`	

Chaves de condição do AWS App Studio

O App Studio não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS App2Container

AWS O App2Container (prefixo do serviço:`a2c`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS App2Container
- Tipos de recursos definidos pelo AWS App2Container
- Chaves de condição para o AWS App2Container

Ações definidas pelo AWS App2Container

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos

("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetContainerizationJobDetails	Concede permissão para obter os detalhes de todos os trabalhos de conteinerização	Leitura			
GetDeploymentJobDetails	Concede permissão para obter os detalhes de todos os trabalhos de implantação	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartContainerizationJob	Concede permissão para iniciar um trabalho de conteinerização	Gravar			
StartDeploymentJob	Concede permissão para iniciar um trabalho de implantação	Gravar			

Tipos de recursos definidos pelo AWS App2Container

AWS O App2Container não suporta a especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para permitir acesso ao AWS App2Container, especifique `"Resource": "*"` na sua política.

Chaves de condição para o AWS App2Container

O App2Container não tem chaves de contexto específicas do serviço que possam ser usadas no elemento `Condition` de instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o AWS AppConfig

AWS AppConfig (prefixo do serviço:`appconfig`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS AppConfig
- Tipos de recursos definidos pelo AWS AppConfig
- Chaves de condição do AWS AppConfig

Ações definidas pelo AWS AppConfig

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de

recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateApplication	Concede permissão para criar um aplicativo	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfigurationProfile	Concede permissão para criar um perfil de configuração	Write	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeploymentStrategy	Concede permissão para criar uma estratégia de implantação	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironment	Concede permissão para criar um ambiente	Gravar	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExtension	Concede permissão para criar uma extensão	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateExtensionAssociation	Concede permissão para criar uma associação de extensão	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateHostedConfigurationVersion	Concede permissão para criar uma versão de configuração hospedada	Write	application*		
			configurationprofile*		
DeleteApplication	Concede permissão para excluir um aplicativo	Write	application*		
DeleteConfigurationProfile	Concede permissão para excluir um perfil de configuração	Write	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			configurationprofile*		
DeleteDeploymentStrategy	Concede permissão para excluir uma estratégia de implantação	Write	deploymentstrategy*		
DeleteEnvironment	Concede permissão para excluir um ambiente	Gravar	application*		
			environment*		
DeleteExtension	Concede permissão para excluir uma extensão	Gravar	extension*		
DeleteExtensionAssociation	Concede permissão para excluir uma associação de extensão	Gravar	extensionassociation*		
DeleteHostedConfigurationVersion	Concede permissão para excluir uma versão de configuração hospedada	Gravar	application*		
			configurationprofile*		
			hostedconfigurationversion*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAccountSettings	Concede permissão para visualizar as configurações de toda a conta AppConfig	Leitura			
GetApplication	Concede permissão para visualizar detalhes sobre um aplicativo	Read	application*		
				aws:ResourceTag/${TagKey}	
GetConfiguration	Concede permissão para visualizar detalhes sobre uma configuração	Read	application*		
			configurationprofile*		
			environment*		
				aws:ResourceTag/${TagKey}	
GetConfigurationProfile	Concede permissão para visualizar detalhes sobre um perfil de configuração	Read	application*		
			configurationprofile*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
GetDeployment	Concede permissão para visualizar detalhes sobre uma implantação	Read	application*		
			deployment*		
			environment*		
				aws:ResourceTag/${TagKey}	
GetDeploymentStrategy	Concede permissão para visualizar detalhes sobre uma estratégia de implantação	Read	deploymentstrategy*		
				aws:ResourceTag/${TagKey}	
GetEnvironment	Concede permissão para visualizar detalhes sobre um ambiente	Leitura	application*		
			environment*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetExtension	Concede permissão para visualizar detalhes sobre uma extensão	Leitura	extension*		
				aws:ResourceTag/${TagKey}	
GetExtensionAssociation	Concede permissão para visualizar detalhes sobre uma associação de extensão	Leitura	extensionassociation*		
				aws:ResourceTag/${TagKey}	
GetHostedConfigurationVersion	Concede permissão para visualizar detalhes sobre uma versão de configuração hospedada	Leitura	application*		
			configurationprofile*		
			hostedconfigurationversion*		
GetLatestConfiguration	Concede permissão para recuperar uma configuração implantada	Leitura	configuration*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListApplications	Concede permissão para listar os aplicativos em sua conta	List			
ListConfigurationProfiles	Concede permissão para listar os perfis de configuração de um aplicativo	List	application*		
ListDeploymentStrategies	Concede permissão para listar as estratégias de implantação para sua conta	List			
ListDeployments	Concede permissão para listar as implantações para um ambiente	List	application*		
			environment*		
ListEnvironments	Concede permissão para listar os ambientes de um aplicativo	Lista	application*		
ListExtensionAssociations	Concede permissão para listar as associações de extensão na conta	Lista			
ListExtensions	Concede permissão para listar as extensões da conta	Lista			
ListHostedConfigurationVersions	Concede permissão para listar as versões de configuração hospedadas para um perfil de configuração	List	application*		
			configurationprofile*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para visualizar uma lista de etiquetas de recursos para um recurso especificado	Leitura	application		
			configurationprofile		
			deployment		
			deploymentstrategy		
			environment		
			extension		
			extensionassociation		
				aws:ResourceTag/${TagKey}	
StartConfigurationSession	Concede permissão para iniciar uma sessão de configuração	Write	configuration*		
				aws:ResourceTag/${TagKey}	
StartDeployment	Concede permissão para iniciar uma implantação	Write	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			configurationprofile*		
			deploymentstrategy*		
			environment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StopDeployment	Concede permissão para interromper uma implantação	Write	application*		
			deployment*		
			environment*		
TagResource	Concede permissão para marcar um recurso appconfig	Tags	application		
			configuration		
			configurationprofile		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			deployment		
			deploymentstrategy		
			environment		
			extension		
			extensionassociation		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permissão para desmarcar um recurso appconfig	Tags	application		
			configuration		
			configurationprofile		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			deployment		
			deploymentstrategy		
			environment		
			extension		
			extensionassociation		
				aws:TagKeys	
UpdateAccountSettings	Concede permissão para modificar as configurações de toda a conta AppConfig	Gravar			
UpdateApplication	Concede permissão para modificar um aplicativo	Write	application*		
				aws:ResourceTag/${TagKey}	
UpdateConfigurationProfile	Concede permissão para modificar um perfil de configuração	Write	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			configurationprofile*		
				aws:ResourceTag/${TagKey}	
UpdateDeploymentStrategy	Concede permissão para modificar uma estratégia de implantação	Write	deploymentstrategy*		
				aws:ResourceTag/${TagKey}	
UpdateEnvironment	Concede permissão para modificar um ambiente	Gravar	application*		
			environment*		
				aws:ResourceTag/${TagKey}	
UpdateExtension	Concede permissão para modificar uma extensão	Gravar	extension*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateExtensionAssociation	Concede permissão para modificar uma associação de extensão	Gravar	extensionassociation*		
				aws:ResourceTag/${TagKey}	
ValidateConfiguration	Concede permissão para validar uma configuração	Gravar	application*		
			configurationprofile*		

Tipos de recursos definidos pelo AWS AppConfig

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
application	`arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
environment	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/environment/${EnvironmentId}	aws:ResourceTag/${TagKey}
configurationprofile	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/configurationprofile/${ConfigurationProfileId}	aws:ResourceTag/${TagKey}
deploymentstrategy	arn:${Partition}:appconfig:${Region}:${Account}:deploymentstrategy/${DeploymentStrategyId}	aws:ResourceTag/${TagKey}
deployment	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/environment/${EnvironmentId}/deployment/${DeploymentNumber}	aws:ResourceTag/${TagKey}
hostedconfigurationversion	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/configurationprofile/${ConfigurationProfileId}/hostedconfigurationversion/${VersionNumber}	
configuration	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/environment/${EnvironmentId}/configuration/${ConfigurationProfileId}	aws:ResourceTag/${TagKey}
extension	arn:${Partition}:appconfig:${Region}:${Account}:extension/${ExtensionId}/${ExtensionVersionNumber}	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
extension association	`arn:${Partition}:appconfig:${Region}:${Account}:extensionassociation/${ExtensionAssociationId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS AppConfig

AWS AppConfig define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelo conjunto permitido de valores para uma etiqueta especificada	String
aws:ResourceTag/${TagKey}	Filtra o acesso por um par de chave-valor de tag atribuído ao recurso AWS	String
aws:TagKeys	Filtra o acesso por uma lista de chaves da etiqueta que são permitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS AppFabric

AWS AppFabric (prefixo do serviço:`appfabric`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS AppFabric
- Tipos de recursos definidos pelo AWS AppFabric
- Chaves de condição do AWS AppFabric

Ações definidas pelo AWS AppFabric

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de

condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchGetUserAccessTasks	Concede permissão para iniciar tarefas de acesso de usuário para vários usuários	Gravar	appbundle*		
ConnectAppAuthorization	Concede permissão para conectar autorizações de aplicativos	Gravar	appauthorization*		
			appbundle*		
CreateAppAuthorization	Concede permissão para criar autorizações de aplicativos para pacotes de aplicativos	Gravar	appbundle*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAppBundle	Concede permissão para criar pacotes de aplicativos em sua conta	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateIngestion	Concede permissão para criar ingestões para pacotes de aplicativos	Gravar	appbundle*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIngestionDestination	Concede permissão para criar destinos de ingestão para pacotes de aplicativos	Gravar	appbundle*		
			ingestion*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAppAuthorization	Concede permissão para excluir autorizações de aplicativos em um pacote de aplicativos	Gravar	appauthorization*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			appbundle*		
DeleteAppBundle	Concede permissão para excluir pacotes de aplicativos em sua conta	Gravar	appbundle*		
DeleteIngestion	Concede permissão para excluir ingestões em um pacote de apps	Gravar	appbundle*		
			ingestion*		
DeleteIngestionDestination	Concede permissão para excluir destinos em uma ingestão	Gravar	appbundle*		
			ingestion*		
			ingestiondestination*		
GetAppAuthorization	Concede permissão para visualizar detalhes sobre autorizações de aplicativos	Leitura	appauthorization*		
			appbundle*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAppBundle	Concede permissão para visualizar detalhes sobre pacotes de aplicativos	Leitura	appbundle*		
				aws:ResourceTag/${TagKey}	
GetIngestion	Concede permissão para visualizar detalhes sobre ingestões	Leitura	appbundle*		
			ingestion*		
				aws:ResourceTag/${TagKey}	
GetIngestionDestination	Concede permissão para visualizar detalhes sobre destinos de ingestões	Leitura	appbundle*		
			ingestion*		
			ingestiondestination*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAppAuthorizations	Concede permissão para recuperar uma lista de autorizações de aplicativos em um pacote de aplicativos	Lista	appbundle*		
ListAppBundles	Concede permissão para recuperar uma lista de pacotes de aplicativos em sua conta	Lista			
ListIngestionDestinations	Concede permissão para recuperar uma lista de destinos em uma ingestão	Lista	appbundle*		
			ingestion*		
ListIngestions	Concede permissão para recuperar uma lista de ingestões em um pacote de aplicativos	Lista	appbundle*		
ListTagsForResource	Concede permissão para listar tags para AppFabric recursos	Leitura	appauthorization		
			appbundle		
			ingestion		
			ingestiondestination		
StartIngestion	Concede permissão para iniciar ingestões	Gravar	appbundle*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			ingestion*		
StartUserAccessTasks	Concede permissão para iniciar tarefas de acesso de usuário	Gravar	appbundle*		
StopIngestion	Concede permissão para interromper ingestões	Gravar	appbundle*		
			ingestion*		
TagResource	Concede permissão para marcar AppFabric recursos	Tags	appauthorization		
			appbundle		
			ingestion		
			ingestiondestination		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para desmarcar recursos AppFabric	Tags	appauthorization		
			appbundle		
			ingestion		
			ingestiondestination		
				aws:TagKeys	
UpdateAppAuthorization	Concede permissão para atualizar autorizações de aplicativos em pacotes de aplicativos	Gravar	appauthorization*		
			appbundle*		
				aws:ResourceTag/${TagKey}	
UpdateIngestionDestination	Concede permissão para atualizar destinos nas ingestões	Gravar	appbundle*		
			ingestion*		
			ingestiondestination*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pelo AWS AppFabric

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
appbundle	`arn:${Partition}:appfabric:${Region}:${Account}:appbundle/${AppBundleIdentifier}`	aws:ResourceTag/${TagKey}
appauthorization	`arn:${Partition}:appfabric:${Region}:${Account}:appbundle/${AppbundleId}/appauthorization/${AppAuthorizationIdentifier}`	aws:ResourceTag/${TagKey}
ingestion	`arn:${Partition}:appfabric:${Region}:${Account}:appbundle/${AppbundleId}/ingestion/${IngestionIdentifier}`	aws:ResourceTag/${TagKey}
ingestion destination	`arn:${Partition}:appfabric:${Region}:${Account}:appbundle/${AppbundleId}/ingestion/${IngestionIdentifier}/in`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
	`gestiondestination/${IngestionDestinationIdentifier}`	

Chaves de condição do AWS AppFabric

AWS AppFabric define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para a Amazon AppFlow

A Amazon AppFlow (prefixo do serviço:`appflow`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.

- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon AppFlow
- Tipos de recursos definidos pela Amazon AppFlow
- Chaves de condição para a Amazon AppFlow

Ações definidas pela Amazon AppFlow

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelFlowExecutions	Concede permissão para cancelar execuções em andamento de um fluxo da Amazon AppFlow	Gravar	flow*		
CreateConnectorProfile	Concede permissão para criar um perfil de login para ser usado com AppFlow fluxos da Amazon	Gravar			
CreateFlow	Concede permissão para criar um AppFlow fluxo na Amazon	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConnectorProfile	Concede permissão para excluir um perfil de login configurado na Amazon AppFlow	Gravar	connectorprofile*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteFlow	Concede permissão para excluir um AppFlow fluxo da Amazon	Gravar	flow*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeConnector	Concede permissão para descrever um conector registrado na Amazon AppFlow	Leitura	connector*		
DescribeConnectorEntity	Concede permissão para descrever todos os campos de um objeto em um perfil de login configurado na Amazon AppFlow	Leitura	connectorprofile*		
DescribeConnectorFields [somente permissão]	Concede permissão para descrever todos os campos de um objeto em um perfil de login configurado na Amazon AppFlow (somente console)	Leitura	connectorprofile*		
DescribeConnectorProfiles	Concede permissão para descrever todos os perfis de login configurados na Amazon AppFlow	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeConnectors	Concede permissão para descrever todos os conectores suportados pela Amazon AppFlow	Leitura			
DescribeFlow	Concede permissão para descrever um fluxo específico configurado na Amazon AppFlow	Leitura	flow*		
DescribeFlowExecution [somente permissão]	Concede permissão para descrever todas as execuções de fluxo para um fluxo configurado na Amazon AppFlow (somente console)	Leitura	flow*		
DescribeFlowExecutionRecords	Concede permissão para descrever todas as execuções de fluxo para um fluxo configurado na Amazon AppFlow	Leitura	flow*		
DescribeFlows [somente permissão]	Concede permissão para descrever todos os fluxos configurados na Amazon AppFlow (somente console)	Leitura			
ListConnectorEntities	Concede permissão para listar todos os objetos de um perfil de login configurado na Amazon AppFlow	Lista	connectorprofile*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListConnectorFields [somente permissão]	Concede permissão para listar todos os objetos de um perfil de login configurado na Amazon AppFlow (somente console)	Leitura	connectorprofile*		
ListConnectors	Concede permissão para listar todos os conectores compatíveis com a Amazon AppFlow	Lista	connector*		
ListFlows	Concede permissão para listar todos os fluxos configurados na Amazon AppFlow	Lista	flow*		
ListTagsForResource	Concede permissão para listar as etiquetas de um fluxo	Leitura	flow*		
RegisterConnector	Concede permissão para registrar um AppFlow conector Amazon	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
ResetConnectorMetadataCache	Concede permissão para redefinir metadados de entidades conectoras que a Amazon AppFlow armazenou em seu cache	Gravar	connectorprofile*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RunFlow [somente permissão]	Concede permissão para executar um fluxo configurado na Amazon AppFlow (somente console)	Gravar	flow*		
StartFlow	Concede permissão para ativar (para fluxos programados e acionados por eventos) ou executar (para fluxos sob demanda) um fluxo configurado na Amazon AppFlow	Gravar	flow*		
StopFlow	Concede permissão para desativar um fluxo programado ou acionado por eventos configurado na Amazon AppFlow	Gravar	flow*		
TagResource	Concede permissão para marcar um fluxo ou um conector	Tags	connector		
			flow		
				aws:TagKeys aws:RequestTag/${TagKey}	
UnRegisterConnector	Concede permissão para cancelar o registro de um conector na Amazon AppFlow	Gravar	connector*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um fluxo ou um conector	Tags	connector		
			flow		
				aws:TagKeys	
UpdateConnectorProfile	Concede permissão para atualizar um perfil de login configurado na Amazon AppFlow	Gravar	connectorprofile*		
UpdateConnectorRegistration	Concede permissão para atualizar um conector registrado configurado na Amazon AppFlow	Gravar	connector*		
UpdateFlow	Concede permissão para atualizar um fluxo configurado na Amazon AppFlow	Gravar	flow*		
UseConnectorProfile [somente permissão]	Concede permissão para usar um perfil de conector ao criar um fluxo na Amazon AppFlow	Gravar	connectorprofile*		

Tipos de recursos definidos pela Amazon AppFlow

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
connector profile	`arn:${Partition}:appflow:${Region}:${Account}:connectorprofile/${ProfileName}`	
flow	`arn:${Partition}:appflow:${Region}:${Account}:flow/${FlowName}`	aws:ResourceTag/${TagKey}
connector	`arn:${Partition}:appflow:${Region}:${Account}:connector/${ConnectorLabel}`	aws:ResourceTag/${TagKey}

Chaves de condição para a Amazon AppFlow

A Amazon AppFlow define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por conjunto de valores permitido para cada uma das etiquetas	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelo valor-etiqueta associado ao recurso	String
aws:TagKeys	Filtra o acesso por presença de etiquetas obrigatórias na solicitação	ArrayOfString

Ações, recursos e chaves de condição para a Amazon AppIntegrations

A Amazon AppIntegrations (prefixo do serviço:`app-integrations`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon AppIntegrations
- Tipos de recursos definidos pela Amazon AppIntegrations
- Chaves de condição para a Amazon AppIntegrations

Ações definidas pela Amazon AppIntegrations

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou

ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateApplication	Concede permissão para criar uma nova aplicação	Gravar	application*		iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateApplicationAssociation [somente permissão]	Concede permissão para criar um ApplicationAssociation	Gravar	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataIntegration	Concede permissão para criar um novo DataIntegration	Gravar	data-integration*		appflow:DeleteFlow appflow:DescribeCo

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					nnectorProfiles iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy kms:CreateGrant profile:GetDomain profile:GetProfileObjectType s3:GetBucketNotification s3:GetEncryptionConfiguration

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					s3:PutBucketNotification
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDataIntegrationAssociation	Concede permissão para criar um DataIntegrationAssociation	Gravar	data-integration*		appflow:CreateFlow appflow:DeleteFlow appflow:DescribeConnectorEntity appflow:DescribeConnectorProfiles appflow:TagResource appflow:UseConnectorProfile profile:CreateSnapshot profile:GetSnapshot

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataIntegrationSchedule	Concede permissão para criar um cronograma de integração de dados	Gravar	data-integration*		
CreateEventIntegration	Concede permissão para criar um novo EventIntegration	Gravar	event-integration*		iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateEventIntegrationAssociation [somente permissão]	Concede permissão para criar um EventIntegrationAssociation	Gravar	event-integration*		events:PutRule events:PutTargets
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Concede permissão para excluir um Application	Gravar	application*		
				aws:ResourceTag/${TagKey}	
DeleteApplicationAssociation [somente permissão]	Concede permissão para excluir um ApplicationAssociation	Gravar	application-association*		
DeleteDataIntegration	Concede permissão para excluir um DataIntegration	Gravar	data-integration*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteDataIntegrationAssociation [somente permissão]	Concede permissão para excluir um DataIntegrationAssociation	Gravar	data-integration-association*		appflow:CreateFlow appflow:DeleteFlow appflow:DescribeConnectorEntity appflow:DescribeConnectorProfiles appflow:StopFlow appflow:TagResource appflow:UseConnectorProfile
DeleteEventIntegration	Concede permissão para excluir um EventIntegration	Gravar	event-integration*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteEventIntegrationAssociation [somente permissão]	Concede permissão para excluir um EventIntegrationAssociation	Gravar	event-integration-association*		events:DeleteRule events:ListTargetsByRule events:RemoveTargets
GetApplication	Concede permissão para visualizar detalhes sobre a aplicação	Leitura	application*		
				aws:ResourceTag/${TagKey}	
GetDataIntegration	Concede permissão para visualizar detalhes sobre DataIntegrations	Leitura	data-integration*		
				aws:ResourceTag/${TagKey}	
GetDataIntegrationExecution	Concede permissão para obter detalhes sobre a execução de uma integração de dados	Leitura	data-integration*		
GetDataIntegrationSchedule	Concede permissão para obter detalhes sobre um cronograma de integração de dados	Leitura	data-integration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetEventIntegration	Concede permissão para visualizar detalhes sobre EventIntegrations	Leitura	event-integration*		
				aws:ResourceTag/${TagKey}	
ListApplicationAssociations	Concede permissão para listar ApplicationAssociations	Lista			
ListApplications	Concede permissão para listar aplicações	Lista			
ListDataIntegrationAssociations	Concede permissão para listar DataIntegrationAssociations	Lista			
ListDataIntegrationExecutions	Concede permissão para listar as execuções de integração de dados	Lista	data-integration*		
ListDataIntegrationSchedules	Concede permissão para listar cronogramas de integração de dados	Lista	data-integration*		
ListDataIntegrations	Concede permissão para listar DataIntegrations	Lista			
ListEventIntegrationAssociations	Concede permissão para listar EventIntegrationAssociations	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListEventIntegrations	Concede permissão para listar EventIntegrations	Lista			
ListTagsForResource	Concede permissão para listas de tags para um AppIntegration recurso da Amazon	Leitura	application		
			data-integration		
			data-integration-association		
			event-integration		
			event-integration-association		
				aws:ResourceTag/${TagKey}	
StartDataIntegrationExecution	Concede permissão para iniciar uma execução de integração de dados	Gravar	data-integration*		profile:CreateSegmentSnapshot profile:CreateSnapshot

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para marcar um AppIntegration recurso da Amazon	Tags	application		
			application-association		
			data-integration		
			data-integration-association		
			event-integration		
			event-integration-association		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para desmarcar um recurso da Amazon AppIntegration	Tags	application		
			application-association		
			data-integration		
			data-integration-association		
			event-integration		
			event-integration-association		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateApplication	Concede permissão para modificar uma aplicação	Gravar	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
UpdateDataIntegration	Concede permissão para modificar um DataIntegration	Gravar	data-integration*		
				aws:ResourceTag/${TagKey}	
UpdateDataIntegrationAssociation	Concede permissão para modificar um DataIntegrationAssociation	Gravar	data-integration-association*		profile:CreateSnapshot profile:GetSnapshot
				aws:ResourceTag/${TagKey}	
UpdateDataIntegrationSchedule	Concede permissão para atualizar um cronograma de integração de dados	Gravar	data-integration*		
UpdateEventIntegration	Concede permissão para modificar um EventIntegration	Gravar	event-integration*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pela Amazon AppIntegrations

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição para a Amazon AppIntegrations

A Amazon AppIntegrations define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves de etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Application Auto Scaling

AWS O Application Auto Scaling (prefixo do serviço:`application-autoscaling`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Application Auto Scaling

- Tipos de recursos definidos pelo AWS Application Auto Scaling
- Chaves de condição do AWS Application Auto Scaling

Ações definidas pelo AWS Application Auto Scaling

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteScalingPolicy	Concede permissão para excluir uma política de escalabilidade	Gravar	ScalableTarget*		
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
DeleteScheduledAction	Concede permissão para excluir uma ação agendada	Gravar	ScalableTarget*		
				application-autoscaling:service-	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				namespace application-autoscaling:scalable-dimension	
DeregisterScalableTarget	Concede permissão para cancelar o registro de um destino escalável	Gravar	ScalableTarget*		
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
DescribeScalableTargets	Concede permissão para descrever um ou mais destinos escaláveis no namespace especificado	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeScalingActivities	Concede permissão para descrever um conjunto de atividades de escalabilidade ou todas as atividades de escalabilidade no namespace especificado	Leitura			
DescribeScalingPolicies	Concede permissão para descrever um conjunto de políticas de escalabilidade ou todas as políticas de escalabilidade no namespace especificado	Leitura			
DescribeScheduledActions	Concede permissão para descrever um conjunto de ações agendadas ou todas as ações agendadas no namespace especificado	Leitura			
GetPredictiveScalingForecast	Concede permissão para recuperar os dados de previsão de uma política de escalabilidade preditiva	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um destino escalável	Leitura	ScalableTarget*		
PutScalingPolicy	Concede permissão para criar e atualizar uma política de escalabilidade para um destino escalável	Gravar	ScalableTarget*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
PutScheduledAction	Concede permissão para criar e atualizar uma ação agendada para um destino escalável	Gravar	ScalableTarget*		
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RegisterScalableTarget	Concede permissão para registrar AWS ou personalizar recursos como alvos escaláveis com o Application Auto Scaling e para atualizar os parâmetros de configuração usados para gerenciar um alvo escalável	Gravar	ScalableTarget*		application-autoscaling:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
TagResource	Concede permissão para etiquetar um destino escalável	Tags	ScalableTarget*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover etiquetas de um destino escalável	Tags	ScalableTarget*		
				aws:TagKeys	

Tipos de recursos definidos pelo AWS Application Auto Scaling

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
ScalableTarget	`arn:${Partition}:application-autoscaling:${Region}:${Account}:scalable-target/${ResourceId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Application Auto Scaling

AWS O Application Auto Scaling define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
application-autoscaling:scalable-dimension	Filtra o acesso pela dimensão escalável que é passada na solicitação	String
application-autoscaling:service-namespace	Filtra o acesso pelo namespace do serviço que é passado na solicitação	String
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Application Cost Profiler Service

AWS O Application Cost Profiler Service (prefixo do serviço:`application-cost-profiler`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Application Cost Profiler Service
- Tipos de recurso definidos pelo AWS Application Cost Profiler Service
- Chaves de condição do AWS Application Cost Profiler Service

Ações definidas pelo AWS Application Cost Profiler Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteReportDefinition	Concede permissão para excluir a configuração com o relatório específico do Application Cost Profiler, desabilitando efetivamente a geração de relatórios.	Write			
GetReportDefinition	Concede permissão para obter a configuração com uma solicitação específica do relatório do Application Cost Profiler.	Read			
ImportApplicationUsage	Concede permissão para importar o uso da aplicação do S3.	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListReportDefinitions	Concede permissão para obter uma lista das diferentes configurações criadas do relatório do Application Cost Profiler.	Read			
PutReportDefinition	Concede permissão para criar configurações do relatório do Application Cost Profiler.	Write			
UpdateReportDefinition	Concede permissão para atualizar uma configuração existente do relatório do Application Cost Profiler.	Write			

Tipos de recurso definidos pelo AWS Application Cost Profiler Service

AWS O Application Cost Profiler Service não suporta a especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para permitir acesso ao AWS Application Cost Profiler Service, especifique `"Resource": "*"` na política.

Chaves de condição do AWS Application Cost Profiler Service

O Application Cost Profiler não tem chaves de contexto específicas do serviço que possam ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do Application Discovery Arsenal

O Application Discovery Arsenal (prefixo de serviço: `arsenal`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Application Discovery Arsenal
- Tipos de recursos definidos pelo Application Discovery Arsenal
- Chaves de condição do Application Discovery Arsenal

Ações definidas pelo Application Discovery Arsenal

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RegisterOnPremisesAgent [somente permissão]	Concede permissão para registrar os coletores de dados AWS fornecidos no Application Discovery Service	Gravar			

Tipos de recursos definidos pelo Application Discovery Arsenal

O Application Discovery Arsenal não oferece suporte à especificação do ARN de um recurso no elemento `Resource` de uma instrução de política do IAM. Para conceder acesso ao Application Discovery Arsenal, especifique `"Resource": "*"` na política.

Chaves de condição do Application Discovery Arsenal

O Application Discovery Arsenal não tem chaves de contexto específicas do serviço que podem ser usadas no elemento `Condition` das instruções da política. Para ver a lista das chaves de contexto

globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o AWS Application DiscoveryService

AWS O Application Discovery Service (prefixo do serviço:`discovery`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Application Discovery Service
- Tipos de recursos definidos pelo AWS Application Discovery Service
- Chaves de condição para o AWS Application Discovery Arsenal

Ações definidas pelo AWS Application Discovery Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos

("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateConfigurationItemsToApplication	Concede permissão à AssociateConfigurationItemsToApplication API. AssociateConfigurationItemsToApplication associa um ou mais itens de configuração a um aplicativo	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchDeleteAgents	Concede permissão à BatchDeleteAgents API. BatchDeleteAgents exclui um ou mais agents/data coletores associados à sua conta, cada um identificado por seu ID de agente. A exclusão de um coletor de dados não exclui os dados coletados anteriormente	Gravar			
BatchDeleteImportData	Concede permissão à BatchDeleteImportData API. BatchDeleteImportData exclui uma ou mais tarefas de importação do Migration Hub, cada uma identificada por sua ID de importação. Cada tarefa de importação tem um número de registros, que podem identificar servidores ou aplicações	Gravar			
CreateApplication	Concede permissão à CreateApplication API. CreateApplication cria um aplicativo com o nome e a descrição fornecidos	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateTags	Concede permissão à CreateTags API. CreateTags cria uma ou mais tags para itens de configuração. As etiquetas são metadados que ajudam a categorizar ativos de TI. Essa API aceita uma lista de vários itens de configuração	Tags			
DeleteApplications	Concede permissão à DeleteApplications API. DeleteApplications exclui uma lista de aplicativos e suas associações com itens de configuração	Gravar			
DeleteTags	Concede permissão à DeleteTags API. DeleteTags exclui a associação entre itens de configuração e uma ou mais tags. Essa API aceita uma lista de vários itens de configuração	Tags		aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeAgents	Concede permissão à DescribeAgents API. DescribeAgents lista os agentes ou o Conector por ID ou lista todos os agents/Connectors associados ao seu usuário, caso você não tenha especificado um ID	Leitura			
DescribeBatchDeleteConfigurationTask	Concede permissão à DescribeBatchDeleteConfigurationTask API. DescribeBatchDeleteConfigurationTask retorna atributos sobre uma tarefa de exclusão em lote para excluir um conjunto de itens de configuração. O ID da tarefa fornecido deve ser o ID da tarefa recebido da saída de StartBatchDeleteConfigurationTask	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeConfigurations	Concede permissão à DescribeConfigurations API. DescribeConfigurations recupera atributos para uma lista de itens IDs de configuração. Todos os fornecidos IDs devem ser do mesmo tipo de ativo (servidor, aplicativo, processo ou conexão). Os campos de saída são específicos ao tipo de ativo selecionado. Por exemplo, a saída de um item de configuração do servidor inclui uma lista de atributos do servidor, como nome do host, sistema operacional e número de placas de rede	Leitura			
DescribeContinuousExports	Concede permissão à DescribeContinuousExports API. DescribeContinuousExports lista as exportações conforme especificado pelo ID. Todas as exportações contínuas associadas ao seu usuário podem ser listadas se você chamar DescribeContinuousExports como estão, sem passar nenhum parâmetro	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeExportConfigurations	Concede permissão à DescribeExportConfigurations API. DescribeExportConfigurations recupera o status de um determinado processo de exportação. Você pode recuperar o status de até 100 processos	Leitura			
DescribeExportTasks	Concede permissão à DescribeExportTasks API. DescribeExportTasks recuperar o status de uma ou mais tarefas de exportação. Você pode recuperar o status de até 100 tarefas de exportação	Leitura			
DescribeImportTasks	Concede permissão à DescribeImportTasks API. DescribeImportTasks retorna uma série de tarefas de importação para seu usuário, incluindo informações de status, horários IDs, URL do objeto Amazon S3 para o arquivo de importação e muito mais	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeTags	Concede permissão à DescribeTags API. DescribeTags recupera uma lista de itens de configuração marcados com uma tag específica. Ou recupera uma lista de todas as etiquetas atribuídas a um determinado item de configuração	Leitura			
DisassociateConfigurationItemsFromApplication	Concede permissão à DisassociateConfigurationItemsFromApplication API. DisassociateConfigurationItemsFromApplication desassocia um ou mais itens de configuração de um aplicativo	Gravar			
ExportConfigurations	Concede permissão à ExportConfigurations API. ExportConfigurations exporta todos os dados de configuração descobertos para um bucket do Amazon S3 ou um aplicativo que permite que você visualize e avalie os dados. Os dados incluem etiquetas e associações de etiquetas, processos, conexões, servidores e performance do sistema	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetDiscoverySummary	Concede permissão à GetDiscoverySummary API. GetDiscoverySummary recupera um breve resumo dos ativos descobertos	Leitura			
GetNetworkConnectionGraph	Concede permissão à GetNetworkConnectionGraph API. GetNetworkConnectionGraph aceita a lista de entrada de um dos - Endereços IP, IDs de servidor ou IDs de nós. Retorna uma lista de nós e bordas que ajuda o cliente a visualizar o gráfico de conexão de rede. Essa API é usada para visualizar a funcionalidade do gráfico de rede no console MigrationHub	Leitura			
ListConfigurations	Concede permissão à ListConfigurations API. ListConfigurations recupera uma lista de itens de configuração de acordo com os critérios especificados em um filtro. Os critérios de filtro identificam os requisitos de relacionamento	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListServerNeighbors	Concede permissão à ListServerNeighbors API. ListServerNeighbors recupera uma lista de servidores que estão a um salto de rede de um servidor especificado	Lista			
StartBatchDeleteConfigurationTask	Concede permissão à StartBatchDeleteConfigurationTask API. StartBatchDeleteConfigurationTask inicia uma exclusão assíncrona em lote dos seus itens de configuração. Todos os fornecidos IDs devem ser do mesmo tipo de ativo (servidor, aplicativo, processo ou conexão). A saída é um ID de tarefa exclusiva que você pode usar para verificar o progresso das exclusões	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartContinuousExport	Concede permissão à StartContinuousExport API. StartContinuousExport iniciar o fluxo contínuo dos dados descobertos pelo agente no Amazon Athena	Gravar			iam:AttachRolePolicy iam:CreatePolicy iam:CreateRole iam:CreateServiceLinkedRole
StartDataCollectionByAgentIds	Concede permissão à StartDataCollectionByAgentIds API. StartDataCollectionByAgentIds instrui os agentes ou conectores especificados a começarem a coletar dados	Gravar			
StartExportTask	Concede permissão à StartExportTask API. StartExportTask exportar os dados de configuração sobre os itens de configuração e relacionamentos descobertos para um bucket do S3 em um formato especificado	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartImportTask	Concede permissão à StartImportTask API. StartImportTask inicia uma tarefa de importação. O recurso de importação do Migration Hub permite que você importe detalhes do seu ambiente local diretamente AWS sem precisar usar as ferramentas do Application Discovery Service (ADS), como o Discovery Connector ou o Discovery Agent. Isso oferece a você a opção de realizar avaliação e planejamento de migrações diretamente dos dados importados, incluindo a capacidade de agrupar os dispositivos como aplicações e acompanhar seu status de migração	Gravar			discovery:AssociateConfigurationItemsToApplication discovery:CreateApplication discovery:CreateTags discovery:GetDiscoverySummary discovery:ListConfigurations s3:GetObject

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopContinuousExport	Concede permissão à StopContinuousExport API. StopContinuousExport interrompe o fluxo contínuo de dados descobertos pelo agente no Amazon Athena	Gravar			
StopDataCollectionByAgentIds	Concede permissão à StopDataCollectionByAgentIds API. StopDataCollectionByAgentIds instrui os agentes ou conectores especificados a pararem de coletar dados	Gravar			
UpdateApplication	Concede permissão à UpdateApplication API. UpdateApplication atualiza metadados sobre um aplicativo	Gravar			

Tipos de recursos definidos pelo AWS Application Discovery Service

AWS O Application Discovery Service não suporta a especificação de um ARN de recurso `Resource` no elemento de uma declaração de política do IAM. Para conceder acesso ao AWS Application Discovery, especifique `"Resource": "*"` na política.

> **Note**
>
> Para separar o acesso, crie e use AWS contas separadas.

Chaves de condição para o AWS Application Discovery Arsenal

AWS O Application Discovery Service define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Application Migration Service

AWS O Application Migration Service (prefixo do serviço:`mgn`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Application Migration Service
- Tipos de recursos definidos pelo AWS Application Migration Service
- Chaves de condição do AWS Application Migration Service

Ações definidas pelo AWS Application Migration Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ArchiveApplication	Concede permissão para arquivar uma aplicação	Gravar	ApplicationResource*		
ArchiveWave	Concede permissão para arquivar uma onda	Gravar	WaveResource*		
AssociateApplications	Concede permissão para associar aplicações a uma onda	Gravar	ApplicationResource*		
			WaveResource*		
AssociateSourceServers	Concede permissão para associar servidores de origem a uma aplicação	Gravar	ApplicationResource*		
			SourceServerResource*		
BatchCreateVolumeSnapshotGroupForMgn [somente permissão]	Concede permissão para criar grupo de snapshots de volume	Write	SourceServerResource*		
BatchDeleteSnapshotRequestF	Concede permissão para solicitação de snapshot de exclusão em lote	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
orMgn [somente permissão]					
ChangeServerLifeCycleState	Concede permissão para alterar o estado do ciclo de vida do servidor de origem	Gravar	SourceServerResource*		
CreateApplication	Concede permissão para criar um aplicativo	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnector	Concede permissão para criar um conector	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLaunchConfigurationTemplate	Concede permissão para criar um modelo de configuração de inicialização	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateNetworkMigrationDefinition	Concede permissão para criar uma definição de migração de rede	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateReplicationConfigurationTemplate	Concede permissão para criar modelo de configuração de replicação	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateVcenterClientForMgn [somente permissão]	Concede permissão para criar um cliente do vcenter	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWave	Concede permissão para criar uma onda	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Concede permissão para excluir um aplicativo	Gravar	ApplicationResource*		
DeleteConnector	Concede permissão para excluir um conector	Gravar	ConnectorResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteJob	Concede permissão para excluir tarefas	Gravar	JobResource*		
DeleteLaunchConfigurationTemplate	Concede permissão para excluir um modelo de configuração de inicialização	Gravar	LaunchConfigurationTemplateResource*		
DeleteNetworkMigrationDefinition	Concede permissão para excluir uma definição de migração de rede	Gravar	NetworkMigrationDefinitionResource*		
DeleteReplicationConfigurationTemplate	Concede permissão para excluir o modelo de configuração de replicação	Write	ReplicationConfigurationTemplateResource*		
DeleteSourceServer	Concede permissão para excluir o servidor de origem	Write	SourceServerResource*		
DeleteVcenterClient	Concede permissão para excluir o cliente do vcenter	Gravar	VcenterClientResource*		
DeleteWave	Concede permissão para excluir uma onda	Gravar	WaveResource*		
DescribeJobLogItems	Concede permissão para descrever itens de log de tarefas	Read	JobResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeJobs	Concede permissão para descrever tarefas	Lista			
DescribeLaunchConfigurationTemplates	Concede permissão para descrever um modelo de configuração de inicialização	Lista			
DescribeReplicationConfigurationTemplates	Concede permissão para descrever o modelo de configuração de replicação	List			
DescribeReplicationServerAssociationsForMgn [somente permissão]	Concede permissão para descrever associações de servidores de replicação	Read			
DescribeSnapshotRequestsForMgn [somente permissão]	Concede permissão para descrever solicitações de snapshots	Read			
DescribeSourceServers	Concede permissão para descrever servidores de origem	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeVcenterClients	Concede permissão para descrever clientes do vcenter	Lista			
DisassociateApplications	Concede permissão para dissociar aplicações de uma onda	Gravar	ApplicationResource*		
			WaveResource*		
DisassociateSourceServers	Concede permissão para dissociar servidores de origem de uma aplicação	Gravar	ApplicationResource*		
			SourceServerResource*		
DisconnectFromService	Concede permissão para desconectar o servidor de origem do serviço	Write	SourceServerResource*		
FinalizeCutover	Concede permissão para finalizar a transição	Write	SourceServerResource*		
GetAgentCommandForMgn [somente permissão]	Concede permissão para obter o comando do agente	Read	SourceServerResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAgentConfirmedResumeInfoForMgn [somente permissão]	Concede permissão para obter informações de currículo confirmado pelo agente	Read	SourceServerResource*		
GetAgentInstallationAssetsForMgn [somente permissão]	Concede permissão para obter ativos de instalação do agente	Read			
GetAgentReplicationInfoForMgn [somente permissão]	Concede permissão para obter informações de replicação do agente	Read	SourceServerResource*		
GetAgentRuntimeConfigurationForMgn [somente permissão]	Concede permissão para obter configuração de runtime do agente	Read	SourceServerResource*		
GetAgentSnapshotCreditsForMgn [somente permissão]	Concede permissão para obter créditos de snapshots do agente	Read	SourceServerResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetChannelCommandsForMgn [somente permissão]	Concede permissão para obter comandos de canal	Read			
GetLaunchConfiguration	Concede permissão para obter a configuração de execução	Leitura	SourceServerResource*		
GetNetworkMigrationDefinition	Concede permissão para obter uma definição de migração de rede	Leitura	NetworkMigrationDefinitionResource*		
GetNetworkMigrationMapperSegmentConstruct	Concede permissão para obter uma construção de segmento do mapeador de migração de rede	Leitura	NetworkMigrationDefinitionResource*		
GetReplicationConfiguration	Concede permissão para obter a configuração de replicação	Leitura	SourceServerResource*		
GetVcenterClientCommandsForMgn [somente permissão]	Concede permissão para obter comandos de cliente do vcenter	Leitura	VcenterClientResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
InitializeService	Concede permissão para inicializar o serviço	Gravar			iam:AddRoleToInstanceProfile iam:CreateInstanceProfile iam:CreateServiceLinkedRole iam:GetInstanceProfile
IssueClientCertificateForMgn [somente permissão]	Concede permissão para emitir um certificado de cliente	Gravar	SourceServerResource		
ListApplications	Concede permissão para listar resumos de aplicações	Lista			
ListConnectors	Concede permissão para listar conectores	Leitura			
ListExportErrors	Concede permissão para listar os erros de uma tarefa de exportação	Lista	ExportResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListExports	Concede permissão para listar tarefas de exportação	Lista			
ListImportErrors	Concede permissão para listar os erros de uma tarefa de importação	Lista	ImportResource*		
ListImports	Concede permissão para listar as tarefas de importação	Lista			
ListManagedAccounts	Concede permissão para listar contas gerenciadas	Lista			
ListNetworkMigrationAnalyses	Concede permissão para listar análises de migração de rede	Lista	NetworkMigrationDefinitionResource*		
ListNetworkMigrationAnalysisResults	Concede permissão para listar os resultados da análise de migração de rede	Lista	NetworkMigrationDefinitionResource*		
ListNetworkMigrationCodeGenerationSegments	Concede permissão para listar segmentos de geração de código de migração de rede	Lista	NetworkMigrationDefinitionResource*		
ListNetworkMigrationCodeGenerations	Concede permissão para listar gerações de código de migração de rede	Lista	NetworkMigrationDefinitionResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListNetworkMigrationDefinitions	Concede permissão para listar as definições de migração de rede	Lista			
ListNetworkMigrationDeployedStacks	Concede permissão para listar as pilhas implantadas de migração de rede	Lista	NetworkMigrationDefinitionResource*		
ListNetworkMigrationDeployedStacksDeletions	Concede permissão para listar a migração de rede, pilhas implantadas e exclusões	Lista	NetworkMigrationDefinitionResource*		
ListNetworkMigrationDeployments	Concede permissão para listar implantações de migração de rede	Lista	NetworkMigrationDefinitionResource*		
ListNetworkMigrationExecutions	Concede permissão para listar as execuções de migração de rede	Lista	NetworkMigrationDefinitionResource*		
ListNetworkMigrationMapperSegmentConstructs	Concede permissão para listar construções de segmentos do mapeador de migração de rede	Lista	NetworkMigrationDefinitionResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListNetworkMigrationMapperSegments	Concede permissão para listar segmentos do mapeador de migração de rede	Lista	NetworkMigrationDefinitionResource*		
ListNetworkMigrationMappings	Concede permissão para listar mapeamentos de migração de rede	Lista	NetworkMigrationDefinitionResource*		
ListSourceServerActions	Concede permissão para listar documentos de ações do servidor de origem	Lista	SourceServerResource*		
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura			
ListTemplateActions	Concede permissão para listar documentos de ação de modelo de configuração	Lista	LaunchConfigurationTemplateResource*		
ListWaves	Concede permissão para listar resumos de ondas	Lista			
MarkAsArchived	Concede permissão para marcar o servidor de origem como arquivado	Write	SourceServerResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
NotifyAgentAuthenticationForMgn [somente permissão]	Concede permissão para notificar a autenticação do agente	Write	SourceServerResource*		
NotifyAgentConnectedForMgn [somente permissão]	Concede permissão para notificar que o agente está conectado	Write	SourceServerResource*		
NotifyAgentDisconnectedForMgn [somente permissão]	Concede permissão para notificar que o agente está desconectado	Write	SourceServerResource*		
NotifyAgentReplicationProgressForMgn [somente permissão]	Concede permissão para notificar o progresso da replicação do agente	Write	SourceServerResource*		
NotifyVcenterClientStartedForMgn [somente permissão]	Concede permissão para notificar cliente do vcenter iniciado	Gravar	VcenterClientResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PauseReplication	Concede permissão para pausar uma replicação	Gravar	SourceServerResource*		
PutSourceServerAction	Concede permissão para colocar documento de ação de servidor de origem	Gravar	SourceServerResource*		
PutTemplateAction	Concede permissão para colocar documento de ação de modelo de configuração	Gravar	LaunchConfigurationTemplateResource*		
RegisterAgentForMgn [somente permissão]	Concede permissão para registrar o agente	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
RemoveSourceServerAction	Concede permissão para remover documento de ação de servidor de origem	Gravar	SourceServerResource*		
RemoveTemplateAction	Concede permissão para remover documento de ação de modelo de configuração	Gravar	LaunchConfigurationTemplateResource*		
ResumeReplication	Concede permissão para retomar uma replicação	Gravar	SourceServerResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RetryDataReplication	Concede permissão para repetir a replicação	Write	SourceServerResource*		
SendAgentLogsForMgn [somente permissão]	Concede permissão para enviar logs do agente	Write	SourceServerResource*		
SendAgentMetricsForMgn [somente permissão]	Concede permissão para enviar métricas do agente	Write	SourceServerResource*		
SendChannelCommandResultForMgn [somente permissão]	Concede permissão para enviar o resultado do comando do canal	Write			
SendClientLogsForMgn [somente permissão]	Concede permissão para enviar logs de clientes	Write			
SendClientMetricsForMgn [somente permissão]	Concede permissão para enviar métricas de clientes	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SendVcenterClientCommandResultForMgn [somente permissão]	Concede permissão para enviar resultado do comando do cliente do vcenter	Write	VcenterClientResource*		
SendVcenterClientLogsForMgn [somente permissão]	Concede permissão para enviar logs de clientes do vcenter	Write	VcenterClientResource*		
SendVcenterClientMetricsForMgn [somente permissão]	Concede permissão para enviar métricas de clientes do vcenter	Write	VcenterClientResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartCutover	Concede permissão para iniciar a transição	Gravar	SourceServerResource*		ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateSecurityGroup ec2:CreateSnapshot ec2:CreateTags ec2:CreateVolume

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DeleteLaunchTemplateVersions ec2:DeleteSnapshot ec2:DeleteVolume ec2:DescribeAccountAttributes ec2:DescribeAvailabilityZones ec2:DescribeImages ec2:DescribeInstanceAttribute ec2:DescribeInstanceStatus

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSnapshots ec2:DescribeSubnets ec2:DescribeVolumes

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DetachVolume ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate ec2:ReportInstanceStatus ec2:RevokeSecurityGroupEgress ec2:RunInstances ec2:StartInstances ec2:StopInstances ec2:TerminateInstances iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					mgn:ListTagsForResource
				aws:RequestTag/${TagKey} aws:TagKeys	
StartExport	Concede permissão para iniciar uma tarefa de exportação	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeLaunchTemplateVersions mgn:DescribeSourceServers mgn:GetLaunchConfiguration mgn:ListApplications mgn:ListWaves s3:PutObject

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartImport	Concede permissão para criar uma tarefa de importação	Gravar			ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplateVersions ec2:ModifyLaunchTemplate mgn:DescribeSourceServers mgn:GetLaunchConfiguration mgn:ListApplications mgn:ListWaves mgn:TagResource mgn:UpdateLaunchCo

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					nfiguration s3:PutObject

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartNetworkMigrationAnalysis	Concede permissão para iniciar uma análise de migração de rede	Gravar	NetworkMigrationDefinitionResource*		directconnect:DescribeConnections directconnect:DescribeDirectConnectGatewayAssociations directconnect:DescribeDirectConnectGatewayAttachments directconnect:DescribeDirectConnectGateways directconnect:DescribeVirtualGateways directconnect:Desc

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ribeVirtualInterfaces ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInsightsPath ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DeleteNetworkInsightsAnalysis ec2:DeleteNetworkInsightsPath

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DeleteNetworkInterface ec2:DeleteSecurityGroup ec2:DeleteTags ec2:DescribeAvailabilityZones ec2:DescribeCustomerGateways ec2:DescribeInstances ec2:DescribeInternetGateways ec2:DescribeManagedPrefixLists

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DescribeNatGateways ec2:DescribeNetworkAcls ec2:DescribeNetworkInsightsAnalyses ec2:DescribeNetworkInsightsPaths ec2:DescribeNetworkInterfaces ec2:DescribePrefixLists ec2:DescribeRegions ec2:DescribeRouteTables

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeTransitGatewayAttachments ec2:DescribeTransitGatewayConnects ec2:DescribeTransitGatewayPeeringAttachments ec2:DescribeTransitGatewayRouteTables ec2:DescribeTransitGatewayV

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					pcAttachments ec2:DescribeTransitGateways ec2:DescribeVpcEndpointServiceConfigurations ec2:DescribeVpcEndpoints ec2:DescribeVpcPeeringConnections ec2:DescribeVpcs ec2:DescribeVpnConnections ec2:DescribeVpnGateways

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:GetManagedPrefixListEntries ec2:GetTransitGatewayRouteTablePropagations ec2:SearchTransitGatewayRoutes ec2:StartNetworkInsightsAnalysis elasticloadbalancing:DescribeListeners elasticloadbalancing:DescribeLoadBalancerAttributes

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					elasticloadbalancing:DescribeLoadBalancers elasticloadbalancing:DescribeRules elasticloadbalancing:DescribeTags elasticloadbalancing:DescribeTargetGroupAttributes elasticloadbalancing:DescribeTargetGroups elasticloadbalancing:Descri

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					beTargetHealth globalaccelerator:ListAccelerators globalaccelerator:ListCustomRoutingAccelerators globalaccelerator:ListCustomRoutingEndpointGroups globalaccelerator:ListCustomRoutingListeners globalaccelerator:ListCustomRoutingP

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ortMappings globalaccelerator:ListEndpointGroups globalaccelerator:ListListeners network-firewall:DescribeFirewall network-firewall:DescribeFirewallPolicy network-firewall:DescribeResourcePolicy network-firewall:DescribeRuleGroup

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					network-firewall:ListFirewallPolicies network-firewall:ListFirewalls network-firewall:ListRuleGroups tiros:CreateQuery tiros:ExtendQuery tiros:GetQueryAnswer tiros:GetQueryExplanation tiros:GetQueryExtensionAccounts

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartNetworkMigrationCodeGeneration	Concede permissão para iniciar a geração do código de migração de rede	Gravar	NetworkMigrationDefinitionResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartNetworkMigrationDeployedStacksDeletion	Concede permissão para iniciar a exclusão das pilhas implantadas de migração de rede	Gravar	NetworkMigrationDefinitionResource*		ec2:AcceptTransitGatewayVpcAttachment ec2:AssociateNatGatewayAddress ec2:AssociateRouteTable ec2:AssociateSubnetCidrBlock ec2:AssociateTransitGatewayRouteTable ec2:AssociateVpcCidrBlock ec2:AttachInternetGateway

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:DeleteInternetGateway ec2:DeleteLaunchTemplate ec2:DeleteLaunchTemplateVersions ec2:DeleteNatGateway ec2:DeleteNetworkAcl

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DeleteNetworkAclEntry ec2:DeleteNetworkInsightsAnalysis ec2:DeleteNetworkInsightsPath ec2:DeleteNetworkInterface ec2:DeleteRoute ec2:DeleteRouteTable ec2:DeleteSecurityGroup ec2:DeleteSnapshot ec2:DeleteSubnet

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DeleteTransitGateway ec2:DeleteTransitGatewayRoute ec2:DeleteTransitGatewayRouteTable ec2:DeleteTransitGatewayVpcAttachment ec2:DeleteVolume ec2:DeleteVpc ec2:DetachInternetGateway ec2:DetachVolume

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DisableTransitGatewayRouteTablePropagation ec2:DisassociateNatGatewayAddress ec2:DisassociateRouteTable ec2:DisassociateTransitGatewayRouteTable ec2:EnableTransitGatewayRouteTablePropagation ec2:ModifyInstanceAttribute

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:ModifyLaunchTemplate ec2:ModifySubnetAttribute ec2:ModifyTransitGateway ec2:ModifyTransitGatewayVpcAttachment ec2:ModifyVolume ec2:ModifyVpcAttribute ec2:RejectTransitGatewayVpcAttachment ec2:ReleaseAddress

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:ReplaceNetworkAclAssociation ec2:ReplaceNetworkAclEntry ec2:ReplaceRoute ec2:ReplaceTransitGatewayRoute ec2:RevokeSecurityGroupEgress ec2:RevokeSecurityGroupIngress ec2:SearchTransitGatewayRoutes

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartNetworkMigrationDeployment	Concede permissão para iniciar uma implantação de migração de rede	Gravar	NetworkMigrationDefinitionResource*		ec2:AcceptTransitGatewayVpcAttachment ec2:AssociateNatGatewayAddress ec2:AssociateRouteTable ec2:AssociateSubnetCidrBlock ec2:AssociateTransitGatewayRouteTable ec2:AssociateVpcCidrBlock ec2:AttachInternetGateway

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNatGateway ec2:CreateNetworkAcl ec2:CreateNetworkAclEntry ec2:CreateNetworkInsightsPath ec2:CreateNetworkInterface

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:CreateRoute ec2:CreateRouteTable ec2:CreateSecurityGroup ec2:CreateSubnet ec2:CreateTags ec2:CreateTransitGatewayRoute ec2:CreateTransitGatewayRouteTable ec2:CreateTransitGatewayVpcAttachment

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DeleteInternetGateway ec2:DeleteLaunchTemplate ec2:DeleteLaunchTemplateVersions ec2:DeleteNatGateway ec2:DeleteNetworkAcl ec2:DeleteNetworkAclEntry ec2:DeleteNetworkInsightsAnalysis ec2:DeleteNetworkInsightsPath

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DeleteNetworkInterface ec2:DeleteRoute ec2:DeleteRouteTable ec2:DeleteSecurityGroup ec2:DeleteSnapshot ec2:DeleteSubnet ec2:DeleteTransitGateway ec2:DeleteTransitGatewayRoute ec2:DeleteTransitGatewayRouteTable

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DeleteTransitGatewayVpcAttachment ec2:DeleteVolume ec2:DeleteVpc ec2:DescribeAccountAttributes ec2:DescribeAddresses ec2:DescribeAvailabilityZones ec2:DescribeCustomerGateways ec2:DescribeEgressOnlyInter

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					netGateways ec2:DescribeHosts ec2:DescribeImages ec2:DescribeInstanceAttribute ec2:DescribeInstanceStatus ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeInternetGateways ec2:DescribeLaunch

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					TemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeManagedPrefixLists ec2:DescribeNatGateways ec2:DescribeNetworkAcls ec2:DescribeNetworkInsightsAnalyses ec2:DescribeNetworkInsightsPaths ec2:DescribeNetworkInterfaces

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DescribePrefixLists ec2:DescribeRegions ec2:DescribeRouteTables ec2:DescribeSecurityGroupRules ec2:DescribeSecurityGroups ec2:DescribeSnapshots ec2:DescribeSubnets ec2:DescribeTransitGatewayAttachments

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DescribeTransitGatewayConnects ec2:DescribeTransitGatewayPeeringAttachments ec2:DescribeTransitGatewayRouteTables ec2:DescribeTransitGatewayVpcAttachments ec2:DescribeTransitGateways ec2:DescribeVolumes ec2:DescribeVpcEndpointServ

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					iceConfigurations ec2:DescribeVpcEndpoints ec2:DescribeVpcPeeringConnections ec2:DescribeVpcs ec2:DescribeVpnConnections ec2:DescribeVpnGateways ec2:DetachInternetGateway ec2:DetachVolume ec2:DisableTransitGatewayRouteTableP

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ropagation ec2:DisassociateNatGatewayAddress ec2:DisassociateRouteTable ec2:DisassociateTransitGatewayRouteTable ec2:EnableTransitGatewayRouteTablePropagation ec2:GetEbsDefaultKmsKeyId ec2:GetEbsEncryptionByDefault

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:GetManagedPrefixListEntries ec2:GetTransitGatewayRouteTableAssociations ec2:GetTransitGatewayRouteTablePropagations ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate ec2:ModifySubnetAttribute ec2:ModifyTransitGateway

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:ModifyTransitGatewayVpcAttachment ec2:ModifyVolume ec2:ModifyVpcAttribute ec2:RejectTransitGatewayVpcAttachment ec2:ReleaseAddress ec2:ReplaceNetworkAclAssociation ec2:ReplaceNetworkAclEntry ec2:ReplaceRoute

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:ReplaceTransitGatewayRoute ec2:RevokeSecurityGroupEgress ec2:RevokeSecurityGroupIngress ec2:SearchTransitGatewayRoutes ec2:StartNetworkInsightsAnalysis
StartNetworkMigrationMapping	Concede permissão para iniciar um mapeamento de migração de rede	Gravar	NetworkMigrationDefinitionResource*		
StartReplication	Concede permissão para iniciar a replicação	Write	SourceServerResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartTest	Concede permissão para iniciar o teste	Gravar	SourceServerResource*		ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateSecurityGroup ec2:CreateSnapshot ec2:CreateTags ec2:CreateVolume

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DeleteLaunchTemplateVersions ec2:DeleteSnapshot ec2:DeleteVolume ec2:DescribeAccountAttributes ec2:DescribeAvailabilityZones ec2:DescribeImages ec2:DescribeInstanceAttribute ec2:DescribeInstanceStatus

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSnapshots ec2:DescribeSubnets ec2:DescribeVolumes

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DetachVolume ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate ec2:ReportInstanceStatus ec2:RevokeSecurityGroupEgress ec2:RunInstances ec2:StartInstances ec2:StopInstances ec2:TerminateInstances iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					mgn:ListTagsForResource
				aws:RequestTag/${TagKey} aws:TagKeys	
StopReplication	Concede permissão para interromper a replicação	Gravar	SourceServerResource*		
TagResource	Concede permissão para atribuir uma tag de recurso	Marcação	ApplicationResource		
			ConnectorResource		
			ExportResource		
			ImportResource		
			JobResource		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			LaunchConfigurationTemplateResource		
			ReplicationConfigurationTemplateResource		
			SourceServerResource		
			VcenterClientResource		
			WaveResource		
				aws:RequestTag/${TagKey} mgn:CreateAction aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TerminateTargetInstances	Concede permissão para encerrar instâncias de destino	Gravar	SourceServerResource*		ec2:DeleteVolume ec2:DescribeInstances ec2:DescribeVolumes ec2:TerminateInstances
				aws:RequestTag/${TagKey} aws:TagKeys	
UnarchiveApplication	Concede permissão para desarquivar uma aplicação	Gravar	ApplicationResource*		
UnarchiveWave	Concede permissão para desarquivar uma onda	Gravar	WaveResource*		
UntagResource	Concede permissão para desmarcar um recurso	Marcação	ApplicationResource		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			ConnectorResource		
			JobResource		
			LaunchConfigurationTemplateResource		
			ReplicationConfigurationTemplateResource		
			SourceServerResource		
			VcenterClientResource		
			WaveResource		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateAgentBacklogForMgn [somente permissão]	Concede permissão para atualizar o backlog do agente	Write	SourceServerResource*		
UpdateAgentConversionInfoForMgn [somente permissão]	Concede permissão para atualizar informações de conversão do agente	Write	SourceServerResource*		
UpdateAgentReplicationInfoForMgn [somente permissão]	Concede permissão para atualizar informações de replicação do agente	Write	SourceServerResource*		
UpdateAgentReplicationProcessStateForMgn [somente permissão]	Concede permissão para atualizar o estado do processo de replicação do agente	Write	SourceServerResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateAgentSourceProperties ForMgn [somente permissão]	Concede permissão para atualizar as propriedades de origem do agente	Gravar	SourceServerResource*		
UpdateApplication	Concede permissão para atualizar uma aplicação	Gravar	ApplicationResource*		
UpdateConnector	Concede permissão para atualizar um conector	Gravar	ConnectorResource*		
UpdateLaunchConfiguration	Concede permissão para atualizar uma configuração de execução	Gravar	SourceServerResource*		
UpdateLaunchConfigurationTemplate	Concede permissão para atualizar uma configuração de execução	Gravar	LaunchConfigurationTemplateResource*		
UpdateNetworkMigrationDefinition	Concede permissão para atualizar uma definição de migração de rede	Gravar	NetworkMigrationDefinitionResource*		
UpdateNetworkMigrationMapperSegment	Concede permissão para atualizar um segmento do mapeador de migração de rede	Gravar	NetworkMigrationDefinitionResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateNetworkMigrationMapperSegmentConstruct	Concede permissão para atualizar uma construção de segmento do mapeador de migração de rede	Gravar	NetworkMigrationDefinitionResource*		
UpdateReplicationConfiguration	Concede permissão para atualizar a configuração de replicação	Write	SourceServerResource*		
UpdateReplicationConfigurationTemplate	Concede permissão para atualizar o modelo de configuração de replicação	Gravar	ReplicationConfigurationTemplateResource*		
UpdateSourceServer	Concede permissão para atualizar o servidor de origem	Gravar	SourceServerResource*		
UpdateSourceServerReplicationType	Concede permissão para atualizar tipo de replicação do servidor fonte	Gravar	SourceServerResource*		
UpdateWave	Concede permissão para atualizar uma onda	Gravar	WaveResource*		
VerifyClientRoleForMgn [somente permissão]	Concede permissão para verificar a função do cliente	Leitura			

Tipos de recursos definidos pelo AWS Application Migration Service

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Tipos de recursos	ARN	Chaves de condição
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/${TagKey}
ConnectorResource	`arn:${Partition}:mgn:${Region}:${Account}:connector/${ConnectorID}`	aws:ResourceTag/${TagKey}
NetworkMigrationDefinitionResource	`arn:${Partition}:mgn:${Region}:${Account}:network-migration-definition/${NetworkMigrationDefinitionID}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Application Migration Service

AWS O Application Migration Service define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pela presença de pares de chave-valor da etiqueta na solicitação	String

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra acesso pela presença de chaves da etiqueta na solicitação	ArrayOfString
mgn:CreateAction	Filtra o acesso pelo nome de uma ação de API de criação de recurso	String

Ações, recursos e chaves de condição para o Amazon Application Recovery Controller - Zonal Shift

O Amazon Application Recovery Controller - Zonal Shift (prefixo do serviço:`arc-zonal-shift`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Application Recovery Controller - Zonal Shift
- Tipos de recursos definidos pelo Amazon Application Recovery Controller - Zonal Shift
- Chaves de condição para o Amazon Application Recovery Controller - Zonal Shift

Ações definidas pelo Amazon Application Recovery Controller - Zonal Shift

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando

usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelPracticeRun	Concede permissão para cancelar uma corrida prática ativa	Gravar	ALB*		
			NLB*		
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CancelZonalShift	Concede permissão para cancelar uma mudança de zona ativa	Gravar	ALB*		
			NLB*		
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				elasticloadbalancing:ResourceTag/${TagKey}	
CreatePracticeRunConfiguration	Concede permissão para criar uma configuração de execução de prática	Gravar	ALB*		cloudwatch:DescribeAlarms iam:CreateServiceLinkedRole
			NLB*		
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeletePracticeRunConfiguration	Concede permissão para excluir uma configuração de execução de prática	Gravar	ALB*		
			NLB*		
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
GetAutoshiftObserverNotificationStatus	Concede permissão para obter o status de notificação do observador de mudança automática	Leitura			
GetManagedResource	Concede permissão para obter informações sobre um recurso gerenciado	Leitura	ALB*		
			NLB*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ListAutoshifts	Concede permissão para listar turnos automáticos ativos e concluídos	Lista			
ListManagedResources	Concede permissão para listar recursos gerenciados	Lista			
ListZonalShifts	Concede permissão para listar mudanças de zona	Lista			
StartPracticeRun	Concede permissão para iniciar uma corrida prática	Gravar	ALB* NLB*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
StartZonalShift	Concede permissão para iniciar uma mudança de zona	Gravar	ALB*		
			NLB*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
UpdateAutoshiftObserverNotificationStatus	Concede permissão para atualizar o status de notificação do observador de mudança automática	Gravar			
UpdatePracticeRunConfiguration	Concede permissão para atualizar uma configuração de execução de prática	Gravar	ALB*		cloudwatch:DescribeAlarms iam:CreateServiceLinkedRole
			NLB*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
UpdateZonalAutoshiftConfiguration	Concede permissão para atualizar um status de desvio automático zonal	Gravar	ALB* NLB*		iam:CreateServiceLinkedRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
UpdateZonalShift	Concede permissão para atualizar uma mudança de zona existente	Gravar	ALB* NLB*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

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

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

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

Tipos de recursos	ARN	Chaves de condição
		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}

Chaves de condição para o Amazon Application Recovery Controller - Zonal Shift

O Amazon Application Recovery Controller - Zonal Shift define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
arc-zonal-shift:ResourceIdentifier	Filtra o acesso pelo identificador do recurso gerenciado	String

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso gerenciado	String
elasticloadbalancing:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso gerenciado	String

Ações, recursos e chaves de condição para o AWS Application Transformation Service

AWS O Application Transformation Service (prefixo do serviço:`application-transformation`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Application Transformation Service
- Tipos de recursos definidos pelo AWS Application Transformation Service
- Chaves de condição para o AWS Application Transformation Service

Ações definidas pelo AWS Application Transformation Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou

ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetContainerization	Concede permissão para obter os detalhes de todos os trabalhos de conteinerização	Leitura			
GetDeployment	Concede permissão para obter os detalhes de todos os trabalhos de implantação	Leitura			
GetGroupingAssessment	Concede permissão para obter os detalhes de uma operação de avaliação de agrupamento	Leitura			
GetPortingCompatibilityAssessment	Concede permissão para obter operação de compatibilidade de transferência	Leitura			
GetPortingRecommendationAssessment	Concede permissão para obter os detalhes de uma operação de avaliação de recomendação de transferência	Leitura			
GetRuntimeAssessment	Concede permissão para obter os detalhes de uma operação de avaliação de runtime	Leitura			
PutLogData	Concede permissão para enviar logs por push (destinado somente a clientes)	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutMetricData	Concede permissão para enviar dados de métricas por push (destinado somente a clientes)	Gravar			
StartContainerization	Concede permissão para iniciar um trabalho de conteinerização	Gravar			
StartDeployment	Concede permissão para iniciar um trabalho de implantação	Gravar			
StartGroupingAssessment	Concede permissão para iniciar uma operação de avaliação de agrupamento	Gravar			
StartPortingCompatibilityAssessment	Concede permissão para iniciar uma operação de compatibilidade de transferência	Gravar			
StartPortingRecommendationAssessment	Concede permissão para iniciar a operação de avaliação de recomendação de transferência	Gravar			
StartRuntimeAssessment	Concede permissão para iniciar uma operação de avaliação de runtime	Gravar			

Tipos de recursos definidos pelo AWS Application Transformation Service

AWS O Application Transformation Service não suporta a especificação de um ARN de recurso `Resource` no elemento de uma declaração de política do IAM. Para conceder acesso ao AWS Application Transformation Service, especifique `"Resource": "*"` na política.

Chaves de condição para o AWS Application Transformation Service

O Application Transformation Service não possui chaves de contexto específicas ao serviço que possam ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o Amazon AppStream 2.0

O Amazon AppStream 2.0 (prefixo do serviço:`appstream`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon AppStream 2.0
- Tipos de recursos definidos pela Amazon AppStream 2.0
- Chaves de condição para Amazon AppStream 2.0

Ações definidas pela Amazon AppStream 2.0

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateAppBlockBuilderAppBlock	Concede permissão para associar o builder de blocos de aplicações especificado ao bloco de aplicações	Gravar	app-block*		
			app-block-builder*		
				aws:ResourceTag/${TagKey}	
AssociateApplicationFleet	Concede permissão para associar a aplicação específica à frota	Gravar	application*		
			fleet*		
				aws:ResourceTag/${TagKey}	
AssociateApplicationToEntitlement	Concede permissão para associar a aplicação específica à autorização específica	Gravar	stack*		
AssociateFleet	Concede permissão para associar a frota especificada à pilha especificada	Write	fleet*		
			stack*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchAssociateUserStack	Concede permissão para associar os usuários especificados às pilhas especificadas. Os usuários em um grupo de usuários não podem ser atribuídos a pilhas com frotas associadas a um domínio do Active Directory	Write	stack*		
				aws:ResourceTag/${TagKey}	
BatchDisassociateUserStack	Concede permissão para desassociar usuários especificados das pilhas especificadas	Gravar	stack*		
				aws:ResourceTag/${TagKey}	
CopyImage	Concede permissão para copiar a imagem especificada dentro da mesma região ou para uma nova região dentro da mesma Conta da AWS	Gravar	image*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAppBlock	Concede permissão para criar um bloco de aplicações. Os blocos de aplicações armazenam detalhes sobre o disco rígido virtual que contém os arquivos da aplicação em um bucket do S3. Ele também armazena o script de configuração com detalhes sobre como montar o disco rígido virtual. Blocos de aplicações são compatíveis apenas com Frotas elásticas	Gravar		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateAppBlockBuilder	Concede permissão para criar um builder de blocos de aplicações. Um builder de blocos de aplicações é uma máquina virtual usada para criar um bloco de aplicações	Gravar	app-block-builder*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAppBlockBuilderStreamingURL	Concede permissão para criar um URL para iniciar uma sessão de transmissão do builder de blocos de aplicações	Gravar	app-block-builder*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateApplication	Concede permissão para criar uma aplicação na conta de cliente. As aplicações armazenam os detalhes sobre como iniciar aplicações em instâncias de transmissão. Isso só é suportado para frotas elásticas	Gravar	app-block*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateDirectoryConfig	Concede permissão para criar um objeto Directory Config na AppStream versão 2.0. Esse objeto inclui as informações de configuração necessárias para ingressar em frotas e image builders nos domínios do Microsoft Active Directory.	Gravar			
CreateEntitlement	Concede permissão para criar uma autorização para controlar o acesso a aplicações com base nos atributos do usuário	Gravar	stack*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateFleet	Concede permissão para criar uma frota. Uma frota é um grupo de instâncias de streaming do qual os aplicativos são executados e transmitidos para os usuários	Write	fleet*		
			image		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateImageBuilder	Concede permissão para criar um image builder. Um image builder é uma máquina virtual usada para criar uma imagem	Write	image*		
			image-builder*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateImageBuilderStreamingURL	Concede permissão para criar um URL para iniciar uma sessão de transmissão do image builder	Write	image-builder*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateStack	Concede permissão para criar uma pilha para começar a fazer streaming de aplicativos para usuários. Uma pilha consiste em uma frota associada, políticas de acesso de usuário e configurações de armazenamento	Gravar	stack*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStreamingURL	Concede permissão para criar um URL temporário para iniciar uma sessão de streaming AppStream 2.0 para o usuário especificado. Um URL de streaming permite que o streaming de aplicativos seja testado sem a configuração do usuário	Gravar	fleet*		
			stack*		
				aws:ResourceTag/${TagKey}	
CreateThemeForStack	Concede permissão para criar um tema de marca personalizada, que pode incluir um logotipo personalizado, links de sites e outros recursos para exibir aos seus usuários	Gravar	stack*		
CreateUpdatedImage	Concede permissão para atualizar uma imagem existente na conta do cliente	Write	image*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateUsageReportSubscription	Concede permissão para criar uma assinatura de relatório de uso. Relatórios de uso são gerados diariamente	Write			
CreateUser	Concede permissão para criar um novo usuário no grupo de usuários	Write			
DeleteAppBlock	Concede permissão para excluir o bloco de aplicações especificado	Gravar	app-block*		
				aws:ResourceTag/${TagKey}	
DeleteAppBlockBuilder	Concede permissão para excluir o builder de blocos de aplicações especificado e liberar capacidade	Gravar	app-block-builder*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteApplication	Concede permissão para excluir a aplicação especificada	Gravar	application*		
				aws:ResourceTag/${TagKey}	
DeleteDirectoryConfig	Concede permissão para excluir o objeto do Directory Config especificado da AppStream versão 2.0. Esse objeto inclui as informações de configuração necessárias para ingressar em frotas e image builders nos domínios do Microsoft Active Directory.	Gravar			
DeleteEntitlement	Concede permissão para excluir a autorização especificada	Gravar	stack*		
DeleteFleet	Concede permissão para excluir a frota especificada	Write	fleet*		
				aws:ResourceTag/${TagKey}	
DeleteImage	Concede permissão para excluir a imagem especificada. Uma imagem não pode ser excluída quando estiver em uso	Write	image*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteImageBuilder	Concede permissão para excluir o image builder especificado e liberar capacidade	Write	image-builder*		
				aws:ResourceTag/${TagKey}	
DeleteImagePermissions	Concede permissão para excluir permissões para a imagem privada especificada	Write	image*		
				aws:ResourceTag/${TagKey}	
DeleteStack	Concede permissão para excluir a pilha especificada. Depois que a pilha for excluída, o ambiente de aplicativo de streaming fornecido pela pilha não estará mais disponível para os usuários. Além disso, quaisquer reservas feitas para as sessões de streaming do aplicativo para a pilha são liberadas	Gravar	stack*		
				aws:ResourceTag/${TagKey}	
DeleteThemeForStack	Concede permissão para excluir um tema de marca personalizada, que pode incluir um logotipo personalizado, links de sites e outros recursos para exibir aos seus usuários	Gravar	stack*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteUsageReportSubscription	Concede permissão para desabilitar a geração de relatórios de uso	Write			
DeleteUser	Concede permissão para excluir um usuário do grupo de usuários	Gravar			
DescribeAppBlockBuilderAppBlockAssociations	Concede permissão para recuperar as associações relacionadas ao builder de blocos de aplicações especificado ou bloco de aplicações	Lista	app-block		
			app-block-builder		
DescribeAppBlockBuilders	Concede permissão para recuperar uma lista que descreve um ou mais builders de blocos de aplicações especificados, caso os nomes de builders de blocos de aplicações sejam fornecidos. Caso contrário, todos os builders de blocos de aplicações na conta serão descritos	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeAppBlocks	Concede permissão para recuperar uma lista que descreve um ou mais blocos de aplicações especificados, se os ARNs de bloco de aplicações são fornecidos. Caso contrário, todos os blocos de aplicações na conta são descritos	Lista			
DescribeApplicationFleetAssociations	Concede permissão para recuperar as associações relacionadas à aplicação ou à frota especificada	Lista	application		
			fleet		
DescribeApplications	Concede permissão para recuperar uma lista que descreve uma ou mais aplicações especificadas, se os nomes de aplicações são fornecidos. Caso contrário, todos as aplicações na conta são descritas	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeDirectoryConfigs	Concede permissão para recuperar uma lista que descreve um ou mais objetos do Directory Config especificados AppStream para 2.0, se os nomes desses objetos forem fornecidos. Caso contrário, todos os objetos Config do diretório na conta são descritos. Esse objeto inclui as informações de configuração necessárias para ingressar em frotas e image builders nos domínios do Microsoft Active Directory.	Lista			
DescribeEntitlements	Concede permissão para recuperar uma ou todas as autorizações para a pilha especificada	Lista	stack*		
DescribeFleets	Concede permissão para recuperar uma lista que descreve uma ou mais frotas especificadas, se os nomes de frota são fornecidos. Caso contrário, todas as frotas na conta são descritas	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeImageBuilders	Concede permissão para recuperar uma lista que descreve um ou mais image builders especificados, se os nomes de image builders são fornecidos. Caso contrário, todos os image builders na conta são descritos	Lista			
DescribeImagePermissions	Concede permissão para recuperar uma lista que descreve as permissões para compartilhar Conta da AWS IDs em uma imagem privada que você possui	Leitura	image*		
DescribeImages	Concede permissão para recuperar uma lista que descreve uma ou mais imagens especificadas, se os nomes das imagens ou imagens ARNs forem fornecidos. Caso contrário, todas as imagens na conta são descritas	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeSessions	Concede permissão para recuperar uma lista que descreve as sessões de streaming para a pilha e a frota especificadas. Se um ID de usuário é fornecido para a pilha e a frota, somente as sessões de streaming são descritas para esse usuário	Lista	fleet* stack*		
DescribeStacks	Concede permissão para recuperar uma lista que descreve uma ou mais pilhas especificadas, se os nomes de pilha são fornecidos. Caso contrário, todas as pilhas na conta são descritas	Lista			
DescribeThemeForStack	Concede permissão para obter as informações do tema de marca personalizada, o que pode incluir um logotipo personalizado, links de sites e outros recursos para exibir aos seus usuários	Leitura	stack*		
DescribeUsageReportSubscriptions	Concede permissão para recuperar uma lista que descreve um ou mais assinaturas de relatório de uso	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeUserStackAssociations	Concede permissão para recuperar uma lista que descreve os objetos UserStackAssociation	Lista	stack		
DescribeUsers	Concede permissão para recuperar uma lista que descreve os usuários no grupo de usuários	Lista			
DisableUser	Concede permissão para desabilitar o usuário especificado no grupo de usuários. Essa ação não exclui o usuário	Gravar			
DisassociateAppBlockBuilderAppBlock	Concede permissão para desassociar o criador de blocos de aplicações especificado do bloco de aplicações	Gravar	app-block*		
			app-block-builder*		
				aws:ResourceTag/${TagKey}	
DisassociateApplicationFleet	Concede permissão para desassociar a aplicação especificada da frota especificada	Gravar	application*		
			fleet*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
DisassociateApplicationFromEntitlement	Concede permissão para desassociar a aplicação especificada da autorização especificada	Gravar	stack*		
DisassociateFleet	Concede permissão para desassociar a frota especificada da pilha especificada	Write	fleet*		
			stack*		
				aws:ResourceTag/${TagKey}	
EnableUser	Concede permissão para habilitar um usuário no grupo de usuários	Write			
ExpireSession	Concede permissão para interromper imediatamente a sessão de streaming especificada	Write			
ListAssociatedFleets	Concede permissão para recuperar o nome da frota associada à pilha especificada	Read	stack*		
ListAssociatedStacks	Concede permissão para recuperar o nome da pilha à qual a frota especificada está associada	Leitura	fleet*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListEntitledApplications	Concede permissão para recuperar as aplicações associadas à autorização especificada	Lista	stack*		
ListTagsForResource	Concede permissão para recuperar uma lista de todas as tags do recurso AppStream 2.0 especificado. Os seguintes recursos podem ser marcados: image builders, imagens, frotas e pilhas	Leitura			
StartAppBlockBuilder	Concede permissão para iniciar o builder de blocos de aplicações especificado	Gravar	app-block-builder*		
				aws:ResourceTag/${TagKey}	
StartFleet	Concede permissão para iniciar a frota especificada	Write	fleet*		
				aws:ResourceTag/${TagKey}	
StartImageBuilder	Concede permissão para iniciar o image builder especificado	Gravar	image-builder*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopAppBlockBuilder	Concede permissão para interromper o builder de blocos de aplicações especificado	Gravar	app-block-builder*		
				aws:ResourceTag/${TagKey}	
StopFleet	Concede permissão para parar a frota especificada	Write	fleet*		
				aws:ResourceTag/${TagKey}	
StopImageBuilder	Concede permissão para parar o image builder especificado	Write	image-builder*		
				aws:ResourceTag/${TagKey}	
Stream	Concede permissão para usuários federados fazerem login usando suas credenciais existentes e fazerem streaming de aplicativos da pilha especificada	Gravar	stack*		
				appstream:userId	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para adicionar ou substituir uma ou mais tags para o recurso AppStream 2.0 especificado. Os seguintes recursos podem ser marcados: image builders, imagens, frotas, pilhas, blocos de aplicações e aplicações	Tags	app-block		
			app-block-builder		
			application		
			fleet		
			image		
			image-builder		
			stack		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
UntagResource	Concede permissão para desassociar uma ou mais tags do recurso AppStream 2.0 especificado	Tags	app-block		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			app-block-builder		
			application		
			fleet		
			image		
			image-builder		
			stack		
				aws:TagKeys	
UpdateAppBlockBuilder	Concede permissão para atualizar um builder de blocos de aplicações específico. Um builder de blocos de aplicações é uma máquina virtual usada para criar um bloco de aplicações	Gravar	app-block-builder*		
				aws:ResourceTag/${TagKey}	
UpdateApplication	Concede permissão para atualizar os campos especificados para a aplicação especificada	Gravar	application*		
			app-block		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
UpdateDirectoryConfig	Concede permissão para atualizar o objeto do Directory Config especificado na AppStream versão 2.0. Esse objeto inclui as informações de configuração necessárias para ingressar em frotas e image builders nos domínios do Microsoft Active Directory.	Gravar			
UpdateEntitlement	Concede permissão para atualizar os campos especificados para a autorização especificada	Gravar	stack*		
UpdateFleet	Concede permissão para atualizar a frota especificada. Todos os atributos, exceto o nome da frota, podem ser atualizados quando a frota estiver no estado STOPPED	Write	fleet*		
			image		
				aws:ResourceTag/${TagKey}	
UpdateImagePermissions	Concede permissão para adicionar ou atualizar as permissões para a imagem privada especificada	Write	image*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateStack	Concede permissão para atualizar os campos especificados para a pilha especificada	Gravar	stack*		
				aws:ResourceTag/${TagKey}	
UpdateThemeForStack	Concede permissão para atualizar as informações do tema de marca personalizada, o que pode incluir um logotipo personalizado, links de sites e outros recursos para exibir aos seus usuários	Gravar	stack*		

Tipos de recursos definidos pela Amazon AppStream 2.0

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
fleet	`arn:${Partition}:appstream:${Region}:${Account}:fleet/${FleetName}`	aws:ResourceTag/${TagKey}
image	`arn:${Partition}:appstream:${Region}:${Account}:image/${ImageName}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição para Amazon AppStream 2.0

A Amazon AppStream 2.0 define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
appstream:userId	Filtra o acesso pelo ID do usuário AppStream 2.0	String

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS AppSync

AWS AppSync (prefixo do serviço:`appsync`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS AppSync
- Tipos de recursos definidos pelo AWS AppSync
- Chaves de condição do AWS AppSync

Ações definidas pelo AWS AppSync

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateApi	Concede permissão para anexar uma API GraphQL a um nome de domínio personalizado no AppSync	Gravar	domain*		
AssociateMergedGraphqlApi	Concede permissão para associar uma API mesclada a uma API de origem	Gravar	graphqlapi*		
AssociateSourceGraphqlApi	Concede permissão para associar uma API de origem a uma API mesclada	Gravar	graphqlapi*		
CreateApi	Concede permissão para criar uma API	Gravar		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole
CreateApiCache	Concede permissão para criar um cache de API no AppSync	Gravar			
CreateApiKey	Concede permissões para criar uma chave exclusiva que você pode distribuir para clientes que estão executando sua API	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateChannelNamespace	Concede permissão para criar um namespace de canal	Gravar	channelNamespace*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSource	Concede permissão para criar uma fonte de dados	Gravar			
CreateDomainName	Concede permissão para criar um nome de domínio personalizado no AppSync	Gravar		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateFunction	Concede permissões para criar um novo objeto function	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateGraphqlApi	Concede permissão para criar uma API GraphQL, que é o recurso de nível superior AppSync	Gravar		aws:RequestTag/${TagKey} aws:TagKeys appsync:Visibility	iam:CreateServiceLinkedRole
CreateResolver	Concede permissão para criar um resolvedor. Um resolvedor converte solicitações de entrada em um formato que uma fonte de dados pode compreender e converte as respostas da fonte de dados em GraphQL	Gravar			
CreateType	Concede permissão para criar um tipo	Gravar			
DeleteApi	Concede permissão para excluir uma API. Isso também limpará todos os AppSync recursos abaixo dessa API	Gravar	api*		
				aws:ResourceTag/${TagKey}	
DeleteApiCache	Concede permissão para excluir um cache de API no AppSync	Gravar			
DeleteApiKey	Concede permissão para excluir uma chave de API	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteChannelNamespace	Concede permissão para excluir um namespace do canal	Gravar	channelNamespace*		
				aws:ResourceTag/${TagKey}	
DeleteDataSource	Concede permissão para excluir uma fonte de dados	Gravar			
DeleteDomainName	Concede permissão para excluir um nome de domínio personalizado no AppSync	Gravar	domain*		
				aws:ResourceTag/${TagKey}	
DeleteFunction	Concede permissão para excluir uma função	Gravar			
DeleteGraphqlApi	Concede permissões para excluir uma Api GraphQL. Isso também limpará todos os AppSync recursos abaixo dessa API	Gravar	graphqlapi*		
				aws:ResourceTag/${TagKey}	
DeleteResolver	Concede permissão para excluir um resolvedor	Gravar			
DeleteResourcePolicy [somente permissão]	Concede permissão para remover uma política de recurso	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteType	Concede permissão para excluir um tipo	Gravar			
DisassociateApi	Concede permissão para separar uma API GraphQL a um nome de domínio personalizado no AppSync	Gravar	domain*		
DisassociateMergedGraphqlApi	Concede permissão para remover uma API de origem associada de uma API mesclada identificada pela API de origem	Gravar	mergedApiAssociation*		
DisassociateSourceGraphqlApi	Concede permissão para remover uma API de origem associada de uma API mesclada identificada pela API mesclada	Gravar	sourceApiAssociation*		
EvaluateCode	Concede permissão para avaliar o código com um runtime e contexto	Leitura			
EvaluateMappingTemplate	Concede permissão para avaliar um mapeamento de modelo	Leitura			
EventConnect	Concede permissão para se conectar a uma API de eventos	Gravar	api*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
EventPublish	Concede permissão para publicar eventos em um namespace do canal	Gravar	channelNamespace*		
EventSubscribe	Concede permissão para se inscrever em um namespace de canal	Gravar	channelNamespace*		
FlushApiCache	Concede permissão para liberar um cache de API em AppSync	Gravar			
GetApi	Concede permissão para recuperar uma API	Leitura	api*		
				aws:ResourceTag/${TagKey}	
GetApiAssociation	Concede permissão para ler o nome de domínio personalizado - detalhes da associação da API GraphQL em AppSync	Leitura	domain*		
GetApiCache	Concede permissão para ler informações sobre um cache de API no AppSync	Leitura			
GetChannelNamespace	Concede permissão para recuperar um namespace de canal	Leitura	channelNamespace*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetDataSource	Concede permissão para recuperar uma origem dos dados	Leitura			
GetDataSourceIntrospection	Concede permissão para recuperar uma introspecção de fonte de dados	Leitura			
GetDomainName	Concede permissão para ler informações sobre um nome de domínio personalizado no AppSync	Leitura	domain*		
				aws:ResourceTag/${TagKey}	
GetFunction	Concede permissão para recuperar uma função	Leitura			
GetGraphqlApi	Concede permissão para recuperar uma API GraphQL	Leitura	graphqlapi*		
				aws:ResourceTag/${TagKey}	
GetGraphqlApiEnvironmentVariables	Concede permissão para recuperar as variáveis de ambiente de uma API GraphQL	Leitura			
GetIntrospectionSchema	Concede permissão para recuperar o esquema de introspecção de uma API GraphQL	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetResolver	Concede permissão para recuperar um resolvedor	Leitura			
GetResourcePolicy [somente permissão]	Concede permissão para ler uma política de recurso	Leitura			
GetSchemaCreationStatus	Concede permissão para recuperar o status atual de uma operação de criação de esquema	Leitura			
GetSourceApiAssociation	Concede permissão para ler informações sobre uma API de origem associada à API mesclada	Leitura	sourceApiAssociation*		
GetType	Concede permissão para recuperar um tipo	Leitura			
GraphQL [somente permissão]	Concede permissão para enviar uma consulta GraphQL a uma API GraphQL	Gravar	field*		
			graphqlapi*		
ListApiKeys	Concede permissão para listar as chaves de API para uma determinada API	Lista			
ListApis	Concede permissão para listar APIs	Lista		aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListChannelNamespaces	Concede permissão para listar o namespace do canal	Lista	api*		
				aws:ResourceTag/${TagKey}	
ListDataSources	Concede permissão para listar as origens de dados de uma determinada API	Lista			
ListDomainNames	Concede permissão para enumerar nomes de domínio personalizados no AppSync	Lista		aws:ResourceTag/${TagKey}	
ListFunctions	Concede permissão para listar as funções de uma determinada API	Lista			
ListGraphqlApis	Concede permissão para listar o GraphQL APIs	Lista			
ListResolvers	Concede permissão para listar os resolvedores de uma determinada API e tipo	Lista			
ListResolversByFunction	Concede permissão para listar os resolvedores associados a uma função específica	Lista			
ListSourceApiAssociations	Concede permissão para listar a fonte APIs associada a uma determinada API mesclada	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	api		
			channelNamespace		
			domain		
			graphqlapi		
				aws:ResourceTag/${TagKey}	
ListTypes	Concede permissão para listar os tipos de uma determinada API	Lista			
ListTypesByAssociation	Concede permissão para listar os tipos para uma determinada API mesclada e associação de API de origem	Lista			
PutGraphqlApiEnvironmentVariables	Concede permissão para atualizar as variáveis de ambiente de uma API GraphQL	Gravar			
PutResourcePolicy [somente permissão]	Concede permissão para definir uma política de recursos	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SetWebACL	Concede permissão para definir uma ACL Web	Gerenciamento de permissões			
SourceGraphQL [somente permissão]	Concede permissão para enviar uma consulta GraphQL para uma API de origem de uma API mesclada	Gravar	field* graphqlapi*		
StartDataSourceIntrospection	Concede permissão para introspectar uma fonte de dados	Gravar			
StartSchemaCreation	Concede permissão para adicionar um novo esquema à sua API GraphQL. Esta operação é assíncrona - GetSchemaCreationStatus pode mostrar quando foi concluída	Gravar			
StartSchemaMerge	Concede permissão para iniciar uma mesclagem de esquema para uma determinada API mesclada e API de origem associada	Gravar	sourceApiAssociation*		
TagResource	Concede permissão para marcar um recurso	Marcação	api channelNamespace		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			domain		
			graphqlapi		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso	Tags	api		
			channelNamespace		
			domain		
			graphqlapi		
				aws:TagKeys aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateApi	Concede permissão para atualizar uma API	Gravar	api*		iam:CreateServiceLinkedRole
				aws:ResourceTag/${TagKey}	
UpdateApiCache	Concede permissão para atualizar um cache de API no AppSync	Gravar			
UpdateApiKey	Concede permissão para atualizar uma chave de API para uma determinada API	Gravar			
UpdateChannelNamespace	Concede permissão para atualizar o namespace de um canal	Gravar	channelNamespace*		
				aws:ResourceTag/${TagKey}	
UpdateDataSource	Concede permissão para atualizar uma fonte de dados	Gravar			
UpdateDomainName	Concede permissão para atualizar um nome de domínio personalizado no AppSync	Gravar	domain*		
				aws:ResourceTag/${TagKey}	
UpdateFunction	Concede permissão para atualizar uma função existente	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateGraphqlApi	Concede permissão para atualizar uma API GraphQL	Gravar	graphqlapi*		iam:CreateServiceLinkedRole
				aws:ResourceTag/${TagKey}	
UpdateResolver	Concede permissão para atualizar um resolvedor	Gravar			
UpdateSourceApiAssociation	Concede permissão para atualizar uma associação de API de origem de API mesclada	Gravar	sourceApiAssociation*		
UpdateType	Concede permissão para atualizar um tipo	Gravar			

Tipos de recursos definidos pelo AWS AppSync

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
channelNamespace	`arn:${Partition}:appsync:${Region}:${Account}:apis/${ApiId}/channelNamespace/${ChannelNamespaceName}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS AppSync

AWS AppSync define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
appsync:Visibility	Filtra o acesso pela visibilidade de uma API	String
aws:RequestTag/${TagKey}	Filtra o acesso pelos pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para a mudança de região ARC da Amazon

O switch de região ARC da Amazon (prefixo do serviço:`arc-region-switch`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo switch de região ARC da Amazon
- Tipos de recursos definidos pelo switch de região ARC da Amazon
- Chaves de condição para o switch de região ARC da Amazon

Ações definidas pelo switch de região ARC da Amazon

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa

ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ApprovePlanExecutionStep	Concede permissão para aprovar uma etapa de execução do plano	Gravar	plan*		
CancelPlanExecution	Concede permissão para cancelar a execução de um plano	Gravar	plan*		
CreatePlan	Concede permissão para criar um plano	Gravar	plan*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeletePlan	Concede permissão para excluir um plano	Gravar	plan*		
DeleteResourcePolicy [somente permissão]	Concede permissão para excluir a política de controle de acesso à RAM de um plano	Gerenciamento de permissões			
GetPlan	Concede permissão para obter informações sobre planos em todos Regiões da AWS usando um plano de controle	Leitura	plan*		
GetPlanEvaluationStatus	Concede permissão para obter o status de avaliação de um plano	Leitura	plan*		
GetPlanExecution	Concede permissão para obter detalhes da execução do plano e informações de configuração	Leitura	plan*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetPlanInRegion	Concede permissão para obter informações sobre um plano em um plano específico Região da AWS usando o switch de região (plano de dados regional)	Leitura	plan*		
GetResourcePolicy [somente permissão]	Concede permissão para obter a política de recursos de um plano	Gerenciamento de permissões	plan*		
ListPlanExecutionEvents	Concede permissão para listar eventos de execução do plano	Lista	plan*		
ListPlanExecutions	Concede permissão para listar as execuções do plano	Lista	plan*		
ListPlans	Concede permissão para listar todos os planos Regiões da AWS usando um plano de controle	Lista			
ListPlansInRegion	Concede permissão para listar planos em um plano específico Região da AWS usando o switch de região (plano de dados regional).	Lista			
ListRoute53HealthChecks	Concede permissão para listar as verificações de saúde do Route 53	Lista	plan*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	plan*		
				aws:ResourceTag/${TagKey}	
PutResourcePolicy [somente permissão]	Concede permissão para definir a política de controle de acesso à RAM para um plano	Gerenciamento de permissões			
StartPlanExecution	Concede permissão para iniciar a execução de um plano	Gravar	plan*		
TagResource	Concede permissão para marcar um recurso	Tags	plan*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover etiquetas de um recurso	Tags	plan*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdatePlan	Concede permissão para atualizar um plano	Gravar	plan*		
UpdatePlanExecution	Concede permissão para atualizar a execução de um plano	Gravar	plan*		
UpdatePlanExecutionStep	Concede permissão para atualizar uma etapa de execução do plano	Gravar	plan*		

Tipos de recursos definidos pelo switch de região ARC da Amazon

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
plan	`arn:${Partition}:arc-region-switch:${Region}:${Account}:plan/${ResourceId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o switch de região ARC da Amazon

O switch de região ARC da Amazon define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:ResourceTag/${TagKey}	Filtra o acesso pela chave e valor de uma etiqueta em uma solicitação	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Artifact

AWS O Artifact (prefixo do serviço:`artifact`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Artifact
- Tipos de recursos definidos pelo AWS Artifact
- Chaves de condição do AWS Artifact

Ações definidas pelo AWS Artifact

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de

condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptAgreement	Concede permissão para aceitar um AWS contrato que ainda não foi aceito pela conta do cliente	Gravar	agreement*		
AcceptNdaForAgreement	Concede permissão para aceitar os termos de um documento de NDA para um determinado recurso de contrato	Gravar	agreement*		
GetAccountSettings	Concede permissão para obter as configurações da conta para o Artifact	Leitura			
GetAgreement	Concede permissão para obter um AWS contrato que ainda não foi aceito pela conta do cliente	Leitura	agreement*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetCustomerAgreement	Concede permissão para obter um AWS contrato que foi aceito pela conta do cliente	Leitura	customer-agreement*		
GetNdaForAgreement	Concede permissão para recuperar o documento NDA para um determinado recurso de contrato	Leitura	agreement*		
GetReport	Concede permissão para baixar um relatório	Leitura	report*		
GetReportMetadata	Concede permissão para baixar metadados associados a um relatório	Leitura	report*		
GetTermForReport	Concede permissão para baixar um termo associado a um relatório	Leitura	report*		
ListAgreements	Concede permissão para listar AWS contratos	Lista			
ListCustomerAgreements	Concede permissão para listar recursos do contrato do cliente que foram aceitos pela conta do cliente	Lista			
ListReports	Concede permissão para listar relatórios em sua conta	Lista			
PutAccountSettings	Concede permissão para colocar as configurações da conta para o Artifact	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
Terminate Agreement	Concede permissão para encerrar um contrato de cliente que foi aceito anteriormente pela conta do cliente	Gravar	customer-agreement*		

Tipos de recursos definidos pelo AWS Artifact

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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

Chaves de condição do AWS Artifact

AWS O Artifact define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições

sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
artifact:ReportCategory	Filtra o acesso pelo qual relatórios de categoria são associados	String
artifact:ReportSeries	Filtra o acesso pelo qual relatórios de séries são associados	String

Ações, recursos e chaves de condição do Amazon Athena

O Amazon Athena (prefixo do serviço: `athena`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Athena
- Tipos de recursos definidos pelo Amazon Athena
- Chaves de condição do Amazon Athena

Ações definidas pelo Amazon Athena

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando

usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchGetNamedQuery	Concede permissão para obter informações sobre uma ou mais consultas nomeadas	Leitura	workgroup*		
BatchGetPreparedStatement	Concede permissão para obter informações sobre uma ou mais instruções preparadas	Leitura	workgroup*		
BatchGetQueryExecution	Concede permissão para obter informações sobre uma ou mais execuções de consulta	Leitura	workgroup*		
CancelCapacityReservation	Concede permissão para cancelar uma reserva de capacidade	Gravar	capacity-reservation*		
CancelQueryExecution	Concede permissão para cancelar a execução de uma consulta. Suspenso. Aplica-se somente aos AWS serviços e entidades principais que usam o driver Athena JDBC anterior à versão 1.1.0. Use de StopQueryExecution outra forma	Gravar	workgroup*		
CreateCapacityReservation	Concede permissão para criar uma reserva de capacidade	Gravar	capacity-reservation*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataCatalog	Concede permissão para criar um catálogo de dados	Gravar	datacatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNamedQuery	Concede permissão para criar uma consulta nomeada	Gravar	workgroup*		
CreateNotebook	Concede permissão para criar um bloco de anotações do EMR	Gravar	workgroup*		
CreatePreparedStatement	Concede permissão para criar uma instrução preparada	Gravar	workgroup*		
CreatePresignedNotebookUrl	Concede permissão para criar um url de bloco de anotações pré-assinado	Gravar	workgroup*		
CreateWorkGroup	Concede permissão para criar um grupo de trabalho	Gravar	workgroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCapacityReservation	Concede permissão para excluir uma reserva de capacidade	Gravar	capacity-reservation*		
DeleteDataCatalog	Concede permissão para excluir um catálogo de dados	Gravar	datacatalog*		
DeleteNamedQuery	Concede permissão para excluir uma consulta nomeada especificada	Gravar	workgroup*		
DeleteNotebook	Concede permissão para excluir um bloco de anotações	Gravar	workgroup*		
DeletePreparedStatement	Concede permissão para excluir uma instrução preparada especificada	Gravar	workgroup*		
DeleteWorkGroup	Concede permissão para excluir um grupo de trabalho	Gravar	workgroup*		
ExportNotebook	Concede permissão para exportar um bloco de anotações	Gravar	workgroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetCalculationExecution	Concede permissão para obter a execução de um cálculo	Leitura	workgroup*		
GetCalculationExecutionCode	Concede permissão para obter o código de execução de um cálculo	Leitura	workgroup*		
GetCalculationExecutionStatus	Concede permissão para obter o status de execução de um cálculo	Leitura	workgroup*		
GetCapacityAssignmentConfiguration	Concede permissão para obter informações de atribuição de capacidade para uma reserva de capacidade	Leitura	capacity-reservation*		
GetCapacityReservation	Concede permissão para obter uma reserva de capacidade	Leitura	capacity-reservation*		
GetCatalogs	Concede permissão para habilitar o acesso a bancos de dados e tabelas. Aplica-se somente à política e aos principais AWS serviços gerenciados que usam um driver Athena JDBC versão 1.1.0	Leitura			
GetDataCatalog	Concede permissão para obter um catálogo de dados	Leitura	datacatalog*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetDatabase	Concede permissão para obter um banco de dados para um catálogo de dados	Leitura	datacatalog*		
GetExecutionEngine	Concede permissão para habilitar o acesso ao banco de dados e à tabela especificados. Aplica-se somente à política e aos principais AWS serviços gerenciados que usam um driver Athena JDBC versão 1.1.0	Leitura			
GetExecutionEngines	Concede permissão para habilitar o acesso a bancos de dados e tabelas. Aplica-se somente à política e aos principais AWS serviços gerenciados que usam um driver Athena JDBC versão 1.1.0	Leitura			
GetNamedQuery	Concede permissão para obter informações sobre a consulta nomeada especificada	Leitura	workgroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetNamespace	Concede permissão para habilitar o acesso ao banco de dados e à tabela especificados. Aplica-se somente à política e aos principais AWS serviços gerenciados que usam um driver Athena JDBC versão 1.1.0	Leitura			
GetNamespaces	Concede permissão para habilitar o acesso a bancos de dados e tabelas. Aplica-se somente à política e aos principais AWS serviços gerenciados que usam um driver Athena JDBC versão 1.1.0	Leitura			
GetNotebookMetadata	Concede permissão para obter metadados de bloco de anotações	Leitura	workgroup*		
GetPreparedStatement	Concede permissão para obter informações sobre a instrução preparada especificada	Leitura	workgroup*		
GetQueryExecution	Concede permissão para obter informações sobre a execução da consulta nomeada especificada	Leitura	workgroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetQueryExecutions	Concede permissão para obter execuções de consulta. Suspenso. Aplica-se somente aos AWS serviços e entidades principais que usam o driver Athena JDBC anterior à versão 1.1.0. Use de ListQueryExecutions outra forma	Leitura			
GetQueryResults	Concede permissão para obter os resultados da consulta	Leitura	workgroup *		
GetQueryResultsStream	Concede permissão para obter a transmissão de resultados da consulta	Leitura	workgroup *		
GetQueryRuntimeStatistics	Concede permissão para obter estatísticas de runtime com relação à execução da consulta especificada	Leitura	workgroup *		
GetSession	Concede permissão para obter uma sessão	Leitura	workgroup *		
GetSessionStatus	Concede permissão para obter o status de uma sessão	Leitura	workgroup *		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetTable	Concede permissão para permitir o acesso à tabela especificada. Aplica-se somente à política e aos principais AWS serviços gerenciados que usam um driver Athena JDBC versão 1.1.0	Leitura			
GetTableMetadata	Concede permissão para obter metadados sobre uma tabela para um catálogo de dados	Leitura	datacatalog*		
GetTables	Concede permissão para habilitar o acesso a tabelas. Aplica-se somente à política e aos principais AWS serviços gerenciados que usam um driver Athena JDBC versão 1.1.0	Leitura			
GetWorkGroup	Concede permissão para obter um grupo de trabalho	Leitura	workgroup*		
ImportNotebook	Concede permissão para importar um bloco de anotações	Gravar	workgroup*		
ListApplicationDPUSizes	Concede permissão para retornar uma lista de ApplicationRuntimeIds	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListCalculationExecutions	Concede permissão para retornar uma lista de execuções de cálculos	Lista	workgroup*		
ListCapacityReservations	Concede permissão para retornar uma lista de reservas de capacidade para o especificado Conta da AWS	Lista			
ListDataCatalogs	Concede permissão para retornar uma lista de catálogos de dados para o especificado Conta da AWS	Lista			
ListDatabases	Concede permissão para retornar uma lista de bancos de dados para um catálogo de dados	Lista	datacatalog*		
ListEngineVersions	Concede permissão para retornar uma lista de versões do motor athena para o especificado Conta da AWS	Leitura			
ListExecutors	Concede permissão para retornar uma lista de executores	Lista			
ListNamedQueries	Concede permissão para retornar uma lista de consultas nomeadas no Amazon Athena para o especificado Conta da AWS	Lista	workgroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListNotebookMetadata	Concede permissão para retornar uma lista de blocos de anotação para um determinado grupo de trabalho	Lista	workgroup*		
ListNotebookSessions	Concede permissão para retornar uma lista de sessões para um determinado bloco de anotação	Lista	workgroup*		
ListPreparedStatements	Concede permissão para retornar uma lista de instruções preparadas para o grupo de trabalho especificado	Lista	workgroup*		
ListQueryExecutions	Concede permissão para retornar uma lista de execuções de consulta para o especificado Conta da AWS	Leitura	workgroup*		
ListSessions	Concede permissão para retornar uma lista de sessões para um determinado grupo de trabalho	Lista	workgroup*		
ListTableMetadata	Concede permissão para retornar uma lista de metadados de tabela em um banco de dados para um catálogo de dados	Leitura	datacatalog*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para retornar uma lista de etiquetas de um recurso	Leitura	capacity-reservation*		
			datacatalog*		
			workgroup*		
ListWorkGroups	Concede permissão para retornar uma lista de grupos de trabalho para o especificado Conta da AWS	Lista			
PutCapacityAssignmentConfiguration	Concede permissão para atribuir capacidade de uma reserva de capacidade para consultas	Gravar	capacity-reservation*		
			workgroup*		
RunQuery	Concede permissão para executar uma consulta. Suspenso. Aplica-se somente aos AWS serviços e entidades principais que usam o driver Athena JDBC anterior à versão 1.1.0. Use de StartQueryExecution outra forma	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartCalculationExecution	Concede permissão para iniciar a execução de um cálculo	Gravar	workgroup*		
StartQueryExecution	Concede permissão para iniciar uma execução da consulta usando uma consulta SQL fornecida como uma string	Gravar	workgroup*		
StartSession	Concede permissão para iniciar uma sessão	Gravar	workgroup*		
StopCalculationExecution	Concede permissão para interromper a execução de um cálculo	Gravar	workgroup*		
StopQueryExecution	Concede permissão para interromper a execução da consulta especificada	Gravar	workgroup*		
TagResource	Concede permissão para adicionar uma etiqueta a um recurso	Tags	capacity-reservation*		
			datacatalog*		
			workgroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
TerminateSession	Concede permissão para encerrar uma sessão	Gravar	workgroup*		
UntagResource	Concede permissão para remover uma etiqueta de um recurso	Tags	capacity-reservation*		
			datacatalog*		
			workgroup*		
				aws:TagKeys	
UpdateCapacityReservation	Concede permissão para atualizar uma reserva de capacidade	Gravar	capacity-reservation*		
UpdateDataCatalog	Concede permissão para atualizar um catálogo de dados	Gravar	datacatalog*		
UpdateNamedQuery	Concede permissão para atualizar uma consulta nomeada especificada	Gravar	workgroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateNotebook	Concede permissão para atualizar um bloco de anotações	Gravar	workgroup *		
UpdateNotebookMetadata	Concede permissão para atualizar metadados de blocos de anotações	Gravar	workgroup *		
UpdatePreparedStatement	Concede permissão para atualizar uma instrução preparada	Gravar	workgroup *		
UpdateWorkGroup	Concede permissão para atualizar um grupo de trabalho	Gravar	workgroup *		

Tipos de recursos definidos pelo Amazon Athena

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
datacatalog	`arn:${Partition}:athena:${Region}:${Account}:datacatalog/${DataCatalogName}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
workgroup	`arn:${Partition}:athena:${Region}:${Account}:workgroup/${WorkGroupName}`	aws:ResourceTag/${TagKey}
capacity-reservation	`arn:${Partition}:athena:${Region}:${Account}:capacity-reservation/${CapacityReservationName}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Athena

O Amazon Athena define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Audit Manager

AWS O Audit Manager (prefixo do serviço:`auditmanager`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Audit Manager
- Tipos de recursos definidos pelo AWS Audit Manager
- Chaves de condição do AWS Audit Manager

Ações definidas pelo AWS Audit Manager

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateAssessmentReportEvidenceFolder	Concede permissão para associar uma pasta de evidências a um relatório de avaliação no AWS Audit Manager	Gravar	assessment*		
BatchAssociateAssessmentReportEvidence	Concede permissão para associar uma lista de evidências a um relatório de avaliação no AWS Audit Manager	Gravar	assessment*		
BatchCreateDelegationByAssessment	Concede permissão para criar delegações para uma avaliação no AWS Audit Manager	Gravar	assessment*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			assessmentControlSet*		
BatchDeleteDelegationByAssessment	Concede permissão para excluir delegações para uma avaliação no AWS Audit Manager	Gravar	assessment*		
			assessmentControlSet*		
BatchDisassociateAssessmentReportEvidence	Concede permissão para desassociar uma lista de evidências de um relatório de avaliação no AWS Audit Manager	Gravar	assessment*		
BatchImportEvidenceToAssessmentControl	Concede permissão para importar uma lista de evidências para um controle de avaliação no AWS Audit Manager	Gravar	assessmentControlSet*		
CreateAssessment	Concede permissão para criar uma avaliação para ser usada com o AWS Audit Manager	Gravar		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAssessmentFramework	Concede permissão para criar uma estrutura para uso no AWS Audit Manager	Gravar	control*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateAssessmentReport	Concede permissão para criar um relatório de avaliação no AWS Audit Manager	Gravar	assessment*		
CreateControl	Concede permissão para criar um controle a ser usado no AWS Audit Manager	Gravar		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeleteAssessment	Concede permissão para excluir uma avaliação no AWS Audit Manager	Gravar	assessment*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAssessmentFramework	Concede permissão para excluir uma estrutura de avaliação no AWS Audit Manager	Gravar	assessmentFramework*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAssessmentFrameworkShare	Concede permissão para excluir uma solicitação de compartilhamento para uma estrutura personalizada no AWS Audit Manager	Gravar			
DeleteAssessmentReport	Concede permissão para excluir um relatório de avaliação no AWS Audit Manager	Gravar	assessment*		
DeleteControl	Concede permissão para excluir um controle no AWS Audit Manager	Gravar	control*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeregisterAccount	Concede permissão para cancelar o registro de uma conta no AWS Audit Manager	Gravar			
DeregisterOrganizationAdminAccount	Concede permissão para cancelar o registro da conta de administrador delegado para o Audit Manager AWS	Gravar			
DisassociateAssessmentReportEvidenceFolder	Concede permissão para desassociar uma pasta de evidências de um relatório de avaliação no AWS Audit Manager	Gravar	assessment*		
GetAccountStatus	Concede permissão para obter o status de uma conta no AWS Audit Manager	Leitura			
GetAssessment	Concede permissão para criar uma avaliação no AWS Audit Manager	Leitura	assessment*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAssessmentFramework	Concede permissão para obter uma estrutura de avaliação no AWS Audit Manager	Leitura	assessmentFramework*		
GetAssessmentReportUrl	Concede permissão para obter o URL de um relatório de avaliação no AWS Audit Manager	Leitura	assessment*		
GetChangeLogs	Concede permissão para obter registros de alterações para uma avaliação no Audit Manager AWS	Leitura	assessment*		
GetControl	Concede permissão para obter um controle no AWS Audit Manager	Leitura	control*		
GetDelegations	Concede permissão para obter todas as delegações no AWS Audit Manager	Lista			
GetEvidence	Concede permissão para obter evidências do AWS Audit Manager	Leitura	assessmentControlSet*		
GetEvidenceByEvidenceFolder	Concede permissão para obter todas as evidências de uma pasta de evidências no AWS Audit Manager	Leitura	assessmentControlSet*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetEvidenceFileUploadUrl	Concede permissão para obter um URL pré-assinado do Amazon S3 que pode ser usado para fazer upload de um arquivo como evidência manual	Leitura			
GetEvidenceFolder	Concede permissão para obter a pasta de evidências do AWS Audit Manager	Leitura	assessmentControlSet*		
GetEvidenceFoldersByAssessment	Concede permissão para obter as pastas de evidências de uma avaliação no AWS Audit Manager	Leitura	assessment*		
GetEvidenceFoldersByAssessmentControl	Concede permissão para obter as pastas de evidências de um controle de avaliação no AWS Audit Manager	Leitura	assessmentControlSet*		
GetInsights	Concede permissão para obter dados de analytics para todas as avaliações ativas	Leitura			
GetInsightsByAssessment	Concede permissão para obter dados de analytics para uma avaliação ativa específica	Leitura			
GetOrganizationAdminAccount	Concede permissão para obter a conta de administrador delegado no AWS Audit Manager	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetServicesInScope	Concede permissão para colocar os serviços no escopo de uma avaliação no AWS Audit Manager	Leitura			
GetSettings	Concede permissão para definir todas as configurações no AWS Audit Manager	Leitura			
ListAssessmentControlInsightsByControlDomain	Concede permissão para listar dados de analytics para controles em um domínio de controle específico e avaliação ativa	Lista			
ListAssessmentFrameworkShareRequests	Concede permissão para listar todas as solicitações de compartilhamento enviadas ou recebidas para estruturas personalizadas no AWS Audit Manager	Lista			
ListAssessmentFrameworks	Concede permissão para listar todas as estruturas de avaliação no AWS Audit Manager	Lista			
ListAssessmentReports	Concede permissão para listar todos os relatórios de avaliação no AWS Audit Manager	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAssessments	Concede permissão para listar todas as avaliações no AWS Audit Manager	Lista			
ListControlDomainInsights	Concede permissão para listar dados de analytics para domínios de controle em todas as avaliações ativas	Lista			
ListControlDomainInsightsByAssessment	Concede permissão para listar dados de analytics para domínios de controle em uma avaliação ativa específica	Lista			
ListControlInsightsByControlDomain	Concede permissão para listar dados de analytics para controles em um domínio de controle específico em todas as avaliações ativas	Lista			
ListControls	Concede permissão para listar todos os controles no AWS Audit Manager	Lista			
ListKeywordsForDataSource	Concede permissão para listar todas as palavras-chave da fonte de dados no AWS Audit Manager	Lista			
ListNotifications	Concede permissão para listar todas as notificações no AWS Audit Manager	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar tags para um recurso do AWS Audit Manager	Leitura	assessment		
			control		
RegisterAccount	Concede permissão para registrar uma conta no AWS Audit Manager	Gravar			
RegisterOrganizationAdminAccount	Concede permissão para registrar uma conta dentro da organização como administrador delegado do AWS Audit Manager	Gravar			
StartAssessmentFrameworkShare	Concede permissão para criar uma solicitação de compartilhamento para uma estrutura personalizada no AWS Audit Manager	Gravar	assessmentFramework*		
TagResource	Concede permissão para marcar um recurso do AWS Audit Manager	Tags	assessment		
			assessmentFramework		
			control		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para desmarcar um recurso do AWS Audit Manager	Tags	assessment	aws:ResourceTag/${TagKey}	
			assessmentFramework	aws:ResourceTag/${TagKey}	
			control	aws:ResourceTag/${TagKey}	
				aws:TagKeys	
UpdateAssessment	Concede permissão para atualizar uma avaliação no AWS Audit Manager	Gravar	assessment*		
UpdateAssessmentControl	Concede permissão para atualizar um controle de avaliação no AWS Audit Manager	Gravar	assessmentControlSet*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateAssessmentControlSetStatus	Concede permissão para atualizar o status de um controle de avaliação definido no AWS Audit Manager	Gravar	assessmentControlSet*		
UpdateAssessmentFramework	Concede permissão para atualizar uma estrutura de avaliação no AWS Audit Manager	Gravar	assessmentFramework*		
			control*		
UpdateAssessmentFrameworkShare	Concede permissão para atualizar uma solicitação de compartilhamento para uma estrutura personalizada no AWS Audit Manager	Gravar	assessmentFramework*		
UpdateAssessmentStatus	Concede permissão para atualizar o status de uma avaliação no AWS Audit Manager	Gravar	assessment*		
UpdateControl	Concede permissão para atualizar um controle no AWS Audit Manager	Gravar	control*		
UpdateSettings	Concede permissão para atualizar as configurações no AWS Audit Manager	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ValidateAssessmentReportIntegrity	Concede permissão para validar a integridade de um relatório de avaliação no AWS Audit Manager	Leitura			

Tipos de recursos definidos pelo AWS Audit Manager

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS Audit Manager

AWS O Audit Manager define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o Amazon Aurora DSQL

O Amazon Aurora DSQL (prefixo do serviço:`dsql`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Aurora DSQL
- Tipos de recursos definidos pelo Amazon Aurora DSQL

- Chaves de condição para o Amazon Aurora DSQL

Ações definidas pelo Amazon Aurora DSQL

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddPeerCluster [somente permissão]	Concede permissão para adicionar um cluster de mesmo nível a um cluster multirregional	Gravar	Cluster*		dsql:PutMultiRegionProperties
CreateCluster	Concede permissão para criar novos clusters	Gravar	Cluster*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys dsql:WitnessRegion	
DbConnect	Concede permissão para se conectar ao banco de dados	Gravar	Cluster*		
DbConnectAdmin	Concede permissão para se conectar ao banco de dados com a função de administrador. A conexão com	Gravar	Cluster*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	qualquer outra função requer DbConnect permissão				
DeleteCluster	Concede permissão para excluir um cluster e todos os seus dados	Gravar	Cluster*		
GetBackupJob	Concede permissão para obter o status de uma tarefa de backup de cluster do Aurora DSQL	Leitura	Cluster*		
GetCluster	Concede permissão para obter informações sobre um cluster	Leitura	Cluster*		
GetRestoreJob	Concede permissão para obter o status de um trabalho de restauração de cluster do Aurora DSQL	Leitura	Cluster*		
GetVpcEndpointServiceName	Concede permissão para recuperar o nome do serviço do VPC endpoint para um cluster	Leitura	Cluster*		
ListClusters	Concede permissão para recuperar uma lista de clusters	Lista			
ListTagsForResource	Concede permissão para listar todas as tags em um recurso do Aurora DSQL	Leitura	Cluster*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutMultiRegionProperties [somente permissão]	Concede permissão para atualizar as propriedades multirregionais de um cluster	Gravar	Cluster*		
PutWitnessRegion [somente permissão]	Concede permissão para configurar e atualizar a região testemunha de um cluster multirregional	Gravar	Cluster*		dsql:PutMultiRegionProperties
				dsql:WitnessRegion	
RemovePeerCluster [somente permissão]	Concede permissão para remover um cluster de mesmo nível de um cluster multirregional	Gravar	Cluster*		dsql:PutMultiRegionProperties
StartBackupJob	Concede permissão para iniciar um trabalho de backup para um cluster Aurora DSQL	Gravar	Cluster*		
StartRestoreJob	Concede permissão para iniciar um trabalho de restauração para um cluster Aurora DSQL	Gravar	Cluster*		dsql:CreateCluster iam:CreateServiceLinkedRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopBackupJob	Concede permissão para interromper uma tarefa de backup para um cluster Aurora DSQL	Gravar	Cluster*		
StopRestoreJob	Concede permissão para interromper um trabalho de restauração para um cluster Aurora DSQL	Gravar	Cluster*		
TagResource	Concede permissão para adicionar tags aos recursos do Aurora DSQL	Tags	Cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover tags dos recursos do Aurora DSQL	Tags	Cluster*		
				aws:TagKeys	
UpdateCluster	Concede permissão para modificar os atributos do cluster	Gravar	Cluster*		
				dsql:WitnessRegion	

Tipos de recursos definidos pelo Amazon Aurora DSQL

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso

também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
Cluster	`arn:${Partition}:dsql:${Region}:${Account}:cluster/${Identifier}`	aws:ResourceTag/${TagKey}

Chaves de condição para o Amazon Aurora DSQL

O Amazon Aurora DSQL define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por um par de chave valor da etiqueta que é permitido na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra o acesso por uma lista de chaves da etiqueta que são permitidas na solicitação	ArrayOfString
dsql:WitnessRegion	Filtra o acesso por região testemunha de clusters multirregionais	String

Ações, recursos e chaves de condição do AWS Auto Scaling

AWS O Auto Scaling (prefixo do serviço:`autoscaling-plans`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Auto Scaling
- Tipos de recursos definidos pelo AWS Auto Scaling
- Chaves de condição do AWS Auto Scaling

Ações definidas pelo AWS Auto Scaling

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateScalingPlan	Cria um plano de escalabilidade.	Write			
DeleteScalingPlan	Exclui o plano de escalabilidade especificado.	Write			
DescribeScalingPlanResources	Descreve os recursos escaláveis no plano de escalabilidade especificado.	Read			
DescribeScalingPlans	Descreve os planos de escalabilidade especificados	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	ou todos os seus planos de escalabilidade.				
GetScalingPlanResourceForecastData	Recupera os dados previstos para um recurso dimensionável.	Read			
UpdateScalingPlan	Atualiza um plano de escalabilidade.	Write			

Tipos de recursos definidos pelo AWS Auto Scaling

AWS O Auto Scaling não suporta a especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para conceder acesso ao AWS Auto Scaling, especifique `"Resource": "*"` na política.

Chaves de condição do AWS Auto Scaling

O Auto Scaling não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS B2B Data Interchange

AWS O B2B Data Interchange (prefixo do serviço:`b2bi`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS B2B Data Interchange
- Tipos de recursos definidos pelo AWS B2B Data Interchange
- Chaves de condição para o AWS B2B Data Interchange

Ações definidas pelo AWS B2B Data Interchange

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateCapability	Concede permissão para criar um novo recurso	Gravar	transformer		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePartnership	Concede permissão para criar uma parceria	Gravar	capability*		
			profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateProfile	Concede permissão para criar um perfil	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
CreateStarterMappingTemplate	Concede permissão para gerar um modelo inicial JSONATA/XSLT	Gravar	transformer*		
CreateTransformer	Concede permissão para criar um transformador	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteCapability	Concede permissão para excluir um recurso	Gravar	capability*		
DeletePartnership	Concede permissão para excluir uma parceria	Gravar	partnership*		
DeleteProfile	Concede permissão para excluir um perfil	Gravar	profile*		
DeleteTransformer	Concede permissão para excluir um transformador	Gravar	transformer*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GenerateMapping	Concede permissão para gerar um modelo de JSONATA/XSLT mapeamento inicial a partir do Amazon Bedrock	Gravar	transformer*		
GetCapability	Concede permissão para obter um recurso	Leitura	capability*		
GetPartnership	Concede permissão para obter uma parceria	Leitura	partnership*		
GetProfile	Concede permissão para obter um perfil	Leitura	profile*		
GetTransformer	Concede permissão para obter um transformador	Leitura	transformer*		
GetTransformerJob	Concede permissão para obter um trabalho de transformador	Leitura	transformer*		
ListCapabilities	Concede permissão para listar todos os recursos	Lista			
ListPartnerships	Concede permissão para listar todas as parcerias	Lista			
ListProfiles	Concede permissão para listar todos os perfis	Lista			
ListTagsForResource	Concede permissão para listar as tags de um recurso B2Bi	Leitura	capability		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			partnership		
			profile		
			transformer		
ListTransformers	Concede permissão para listar todos os transformadores	Lista			
StartTransformerJob	Concede permissão para transformar um documento	Gravar	transformer*		
TagResource	Concede permissão para atribuir uma tag a um recurso B2Bi	Tags	capability		
			partnership		
			profile		
			transformer		
				aws:TagKeys aws:RequestTag/${TagKey}	
TestConversion	Concede permissão para JSON/XML converter um em um documento edi	Gravar	transformer*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TestMapping	Concede permissão para mapear um arquivo de amostra	Gravar	transformer*		
TestParsing	Concede permissão para analisar um documento edi	Gravar	transformer*		
UntagResource	Concede permissão para remover uma tag de um recurso B2Bi	Tags	capability		
			partnership		
			profile		
			transformer		
				aws:TagKeys	
UpdateCapability	Concede permissão para atualizar um recurso	Gravar	capability*		
			transformer		
UpdatePartnership	Concede permissão para atualizar uma parceria	Gravar	partnership*		
			capability		
UpdateProfile	Concede permissão para atualizar um perfil	Gravar	profile*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateTransformer	Concede permissão para atualizar um transformador	Gravar	transformer*		

Tipos de recursos definidos pelo AWS B2B Data Interchange

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
profile	`arn:${Partition}:b2bi:${Region}:${Account}:profile/${ResourceId}`	aws:ResourceTag/${TagKey}
capability	`arn:${Partition}:b2bi:${Region}:${Account}:capability/${ResourceId}`	aws:ResourceTag/${TagKey}
partnership	`arn:${Partition}:b2bi:${Region}:${Account}:partnership/${ResourceId}`	aws:ResourceTag/${TagKey}
transformer	`arn:${Partition}:b2bi:${Region}:${Account}:transformer/${ResourceId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o AWS B2B Data Interchange

AWS O B2B Data Interchange define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais

as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Backup

AWS O Backup (prefixo do serviço:`backup`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Backup
- Tipos de recursos definidos pelo AWS Backup
- Chaves de condição do AWS Backup

Ações definidas pelo AWS Backup

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateBackupVaultMpaApprovalTeam	Concede permissão para associar uma equipe de aprovação do MPA a um cofre de backup	Gravar	backupVault*		
				backup:MpaApprovalTeamArn	
CancelLegalHold	Concede permissão para cancelar uma retenção legal	Gravar	legalHold*		
CopyFromBackupVault [somente permissão]	Concede permissão para copiar a partir de um cofre de backup	Write	recoveryPoint*		
				backup:CopyTargets backup:CopyTargetOrgPaths	
CopyIntoBackupVault [somente permissão]	Concede permissão para copiar em um cofre de backup	Write	backupVault*		
				aws:RequestTag/${TagKey}	
CreateBackupPlan	Concede permissão para criar um novo plano de backup	Write	backupPlan*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBackupSelection	Concede permissão para criar uma nova atribuição de recurso em um plano de backup	Write	backupPlan*		iam:PassRole
CreateBackupVault	Concede permissão para criar um novo cofre de backup	Gravar	backupVault*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFramework	Concede permissão para criar uma nova framework	Gravar	framework*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLegalHold	Concede permissão para criar uma nova retenção legal	Gravar	legalHold*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLogicallyAirGappedBackupVault	Concede permissão para criar um novo cofre de backup logicamente isolado, um contêiner lógico no qual os backups são armazenados	Gravar	backupVault*		
				aws:RequestTag/${TagKey} aws:TagKeys backup:MinRetentionDays backup:MaxRetentionDays	
CreateReportPlan	Concede permissão para criar um novo plano de relatório	Gravar	reportPlan*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys backup:FrameworkArns	
CreateRestoreAccessBackupVault	Concede permissão para criar um cofre de backup de acesso à restauração	Gravar	backupVault*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRestoreTestingPlan	Concede permissão para criar um novo plano de testes de restauração	Gravar	restoreTestingPlan*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateRestoreTestingSelection	Concede permissão para criar uma nova atribuição de recurso em um plano de testes de restauração	Gravar	restoreTestingPlan*		iam:PassRole
DeleteBackupPlan	Concede permissão para excluir um plano de backup	Write	backupPlan*		
DeleteBackupSelection	Concede permissão para excluir uma atribuição de recurso de um plano de backup	Write	backupPlan*		
DeleteBackupVault	Concede permissão para excluir um cofre de backup	Write	backupVault*		
DeleteBackupVaultAccessPolicy	Concede permissão para excluir a política de acesso ao cofre de backup	Gerenciamento de permissões	backupVault*		
DeleteBackupVaultLockConfiguration	Concede permissão para remover a configuração de bloqueio de um cofre de backup	Gravar	backupVault*		
DeleteBackupVaultNotifications	Concede permissão para remover as notificações de um cofre de backup	Gravar	backupVault*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteBackupVaultSharingPolicy [somente permissão]	Concede permissão para excluir a política de compartilhamento do cofre de backup	Gerenciamento de permissões	backupVault*		
DeleteFramework	Concede permissões para excluir uma framework	Gravar	framework*		
DeleteRecoveryPoint	Concede permissão para excluir um ponto de recuperação de um cofre de backup	Gravar	recoveryPoint*		
DeleteReportPlan	Concede permissão para excluir um plano de relatório	Gravar	reportPlan*		
DeleteRestoreTestingPlan	Concede permissão para excluir um plano de testes de restauração	Gravar	restoreTestingPlan*		
DeleteRestoreTestingSelection	Concede permissão para excluir uma atribuição de recurso de um plano de testes de restauração	Gravar	restoreTestingPlan*		
DescribeBackupJob	Concede permissão para descrever um trabalho de backup	Read			
DescribeBackupVault	Concede permissão para descrever um novo cofre de backup com o nome especificado	Read	backupVault*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeCopyJob	Concede permissão para descrever um trabalho de cópia	Leitura			
DescribeFramework	Concede permissão para descrever uma framework com o nome especificado	Leitura	framework*		
DescribeGlobalSettings	Concede permissão para descrever as configurações globais	Read			
DescribeProtectedResource	Concede permissão para descrever um recurso protegido	Read			
DescribeRecoveryPoint	Concede permissão para descrever um ponto de recuperação	Read	recoveryPoint*		
DescribeRegionSettings	Concede permissão para descrever as configurações da região	Leitura			
DescribeReportJob	Concede permissão para descrever um trabalho de relatório	Leitura			
DescribeReportPlan	Concede permissão para descrever um novo plano de relatório com o nome especificado	Leitura	reportPlan*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeRestoreJob	Concede permissão para descrever um trabalho de restauração	Leitura			
DisassociateBackupVaultMpaApprovalTeam	Concede permissão para desassociar uma equipe de aprovação de MPA de um cofre de backup	Gravar	backupVault*		
DisassociateRecoveryPoint	Concede permissão para desassociar um ponto de recuperação de um cofre de backup	Gravar	recoveryPoint*		
DisassociateRecoveryPointFromParent	Concede permissão para dissociar um ponto de recuperação de seu pai	Gravar	recoveryPoint*		
ExportBackupPlanTemplate	Concede permissão para exportar um plano de backup como JSON	Read			
GetBackupPlan	Concede permissão para obter um plano de backup	Read	backupPlan*		
GetBackupPlanFromJSON	Concede permissão para transformar JSON em um plano de backup	Read			
GetBackupPlanFromTemplate	Concede permissão para transformar um modelo em um plano de backup	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetBackupSelection	Concede permissão para obter uma atribuição de recursos de plano de backup	Read	backupPlan*		
GetBackupVaultAccessPolicy	Concede permissão para obter a política de acesso ao cofre de backup	Read	backupVault*		
GetBackupVaultNotifications	Concede permissão para receber notificações do cofre de backup	Leitura	backupVault*		
GetBackupVaultSharingPolicy [somente permissão]	Concede permissão para obter a política de compartilhamento do cofre de backup	Leitura	backupVault*		
GetLegalHold	Concede permissão para obter uma retenção legal	Leitura	legalHold*		
GetRecoveryPointIndexDetails	Concede permissão para obter detalhes de indexação para um ponto de recuperação	Leitura	recoveryPoint*		
GetRecoveryPointRestoreMetadata	Concede permissão para obter metadados de restauração do ponto de recuperação	Leitura	recoveryPoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetRestoreJobMetadata	Concede permissão para obter os metadados de restauração associados a um trabalho de restauração	Leitura			
GetRestoreTestingInferredMetadata	Concede permissão para obter metadados inferidos gerados pelos testes de restauração	Leitura			
GetRestoreTestingPlan	Concede permissão para obter um plano de testes de restauração	Leitura	restoreTestingPlan *		
GetRestoreTestingSelection	Concede permissão para obter uma atribuição de recurso de um plano de testes de restauração	Leitura	restoreTestingPlan *		
GetSupportedResourceTypes	Concede permissão para obter tipos de recursos compatíveis	Leitura			
ListBackupJobSummaries	Concede permissão para listar resumos de trabalhos de backup	Lista			
ListBackupJobs	Concede permissão para listar trabalhos de backup	Lista			
ListBackupPlanTemplates	Concede permissão para listar modelos de plano de backup fornecidos pelo AWS Backup	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListBackupPlanVersions	Concede permissão para listar versões do plano de backup	Lista	backupPlan*		
ListBackupPlans	Concede permissão para listar os planos de backup	Lista			
ListBackupSelections	Concede permissão para listar atribuições de recursos para um plano de backup específico	Lista	backupPlan*		
ListBackupVaults	Concede permissão para listar os cofres de backup	Lista			
ListCopyJobSummaries	Concede permissão para listar resumos de trabalhos de cópia	Lista			
ListCopyJobs	Concede permissão para listar trabalhos de cópia	Lista			
ListFrameworks	Concede permissão para listar as frameworks	Lista			
ListIndexedRecoveryPoints	Concede permissão para obter pontos de recuperação indexados à lista	Lista			
ListIndexedRecoveryPointsForSearch [somente permissão]	Concede permissão para listar pontos de recuperação indexados para pesquisa	Gerenciamento de permissões			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListLegalHolds	Concede permissão para listar retenções legais	Lista			
ListProtectedResources	Concede permissão para listar recursos protegidos pelo AWS Backup	Lista			
ListProtectedResourcesByBackupVault	Concede permissão para listar recursos protegidos dentro de um cofre de backup	Lista	backupVault*		
ListRecoveryPointsByBackupVault	Concede permissão para listar pontos de recuperação dentro de um cofre de backup	Lista	backupVault*		
ListRecoveryPointsByLegalHold	Concede permissão para listar pontos de recuperação por retenção legal	Lista	legalHold*		
ListRecoveryPointsByResource	Concede permissão para listar pontos de recuperação de um recurso	Lista			
ListReportJobs	Concede permissão para listar os trabalhos de relatório	Lista			
ListReportPlans	Concede permissão para listar os planos de relatório	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListRestoreAccessBackupVaults	Concede permissão para listar cofres de backup de acesso à restauração associados a um cofre de backup	Lista	backupVault*		
ListRestoreJobSummaries	Concede permissão para listar resumos de trabalhos de recuperação	Lista			
ListRestoreJobs	Concede permissão para listar trabalhos de restauração	Lista			
ListRestoreJobsByProtectedResource	Concede permissão para listar trabalhos de restauração para um recurso protegido	Lista			
ListRestoreTestingPlans	Concede permissão para listar os planos de testes de restauração	Lista			
ListRestoreTestingSelections	Concede permissão para listar atribuições de recursos para um plano de testes de restauração específico	Lista	restoreTestingPlan*		
ListTags	Concede permissão para listar as etiquetas de um recurso	Read	backupPlan		
			backupVault		
			framework		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			legalHold		
			recoveryPoint		
			reportPlan		
			restoreTestingPlan		
PutBackupVaultAccessPolicy	Concede permissão para adicionar uma política de acesso ao cofre de backup	Gerenciamento de permissões	backupVault*		
PutBackupVaultLockConfiguration	Concede permissão para adicionar uma configuração de bloqueio ao cofre de backup	Gravar	backupVault*		
				backup:ChangeableForDays backup:MinRetentionDays backup:MaxRetentionDays	
PutBackupVaultNotifications	Concede permissão para adicionar um tópico SNS ao cofre de backup	Gravar	backupVault*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutBackupVaultSharingPolicy [somente permissão]	Concede permissão para adicionar uma política de compartilhamento ao cofre de backup	Gerenciamento de permissões	backupVault*		
PutRestoreValidationResult	Concede permissão para colocar um resultado de validação de restauração	Gravar			
RevokeRestoreAccessBackupVault	Concede permissão para revogar um cofre de backup de acesso à restauração	Gravar	backupVault*		
SearchRecoveryPoint [somente permissão]	Concede permissão para pesquisar um ponto de recuperação	Gerenciamento de permissões	recoveryPoint*		
StartBackupJob	Concede permissão para iniciar um novo trabalho de backup	Write	backupVault*		iam:PassRole
StartCopyJob	Concede permissão para copiar um backup de um cofre de backup de origem para um cofre de backup de destino	Gravar	recoveryPoint*		iam:PassRole
StartReportJob	Concede permissão para iniciar um novo trabalho de relatório	Gravar	reportPlan*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartRestoreJob	Concede permissão para iniciar um novo trabalho de restauração	Write	recoveryPoint*		iam:PassRole
StopBackupJob	Concede permissão para interromper um trabalho de backup	Write			
TagResource	Concede permissão para marcar um recurso	Marcação	backupPlan		
			backupVault		
			framework		
			legalHold		
			recoveryPoint		
			reportPlan		
			restoreTestingPlan		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para desmarcar um recurso	Marcação	backupPlan		
			backupVault		
			framework		
			legalHold		
			recoveryPoint		
			reportPlan		
			restoreTestingPlan		
				aws:TagKeys	
UpdateBackupPlan	Concede permissão para atualizar um plano de backup	Gravar	backupPlan*		
UpdateFramework	Concede permissão para atualizar uma framework	Gravar	framework*		
UpdateGlobalSettings	Concede permissão para atualizar as configurações globais atuais da AWS Conta	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateRecoveryPointIndexSettings	Concede permissão para atualizar as configurações do índice de pontos de recuperação	Gravar	recoveryPoint*		
				backup:Index	
UpdateRecoveryPointLifecycle	Concede permissão para atualizar o ciclo de vida do ponto de recuperação	Write	recoveryPoint*		
UpdateRegionSettings	Concede permissão para atualizar as configurações atuais de opção pelo serviço para a região	Gravar			
UpdateReportPlan	Concede permissão para atualizar um plano de relatório	Gravar	reportPlan*		
				backup:FrameworkArns	
UpdateRestoreTestingPlan	Concede permissão para atualizar um plano de testes de restauração	Gravar	restoreTestingPlan*		
UpdateRestoreTestingSelection	Concede permissão para atualizar uma atribuição de recurso em um plano de testes de restauração	Gravar	restoreTestingPlan*		iam:PassRole

Tipos de recursos definidos pelo AWS Backup

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

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

Chaves de condição do AWS Backup

AWS O Backup define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelo conjunto de valores permitido para cada uma das etiquetas	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra o acesso pela presença de etiquetas obrigatórias na solicitação	ArrayOfString
backup:ChangeableForDays	Filtra o acesso pelo valor do ChangeableForDays parâmetro	Numérico
backup:CopyTargetOrgPaths	Filtra o acesso pela unidade da organização	ArrayOfString
backup:CopyTargets	Filtra o acesso pelo ARN de um cofre de backup	ArrayOfARN
backup:FrameworkArns	Filtra o acesso pelo Framework ARNs	ArrayOfARN
backup:Index	Filtra o acesso pelo valor do parâmetro Index	String

Chaves de condição	Descrição	Tipo
backup:MaxRetentionDays	Filtra o acesso pelo valor do MaxRetentionDays parâmetro	Numérico
backup:MinRetentionDays	Filtra o acesso pelo valor do MinRetentionDays parâmetro	Numérico
backup:MpaApprovalTeamArn	Filtra o acesso pelo ARN da equipe de aprovação do MPA a um cofre de backup	ARN

Ações, recursos e chaves de condição do AWS Backup Gateway

AWS O Backup Gateway (prefixo do serviço:`backup-gateway`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Backup Gateway
- Tipos de recursos definidos pelo AWS Backup Gateway
- Chaves de condição do AWS Backup Gateway

Ações definidas pelo AWS Backup Gateway

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateGatewayToServer	Concede permissão para AssociateGatewayToServer	Gravar	gateway*		
			hypervisor*		
Backup	Concede permissão para Backup	Gravar	virtualmachine*		
CreateGateway	Concede permissão para CreateGateway	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteGateway	Concede permissão para DeleteGateway	Gravar	gateway*		
DeleteHypervisor	Concede permissão para DeleteHypervisor	Gravar	hypervisor*		
DisassociateGatewayFromServer	Concede permissão para DisassociateGatewayFromServer	Gravar	gateway*		
GetBandwidthRateLimitSchedule	Concede permissão para GetBandwidthRateLimitSchedule	Leitura	gateway*		
GetGateway	Concede permissão para GetGateway	Leitura	gateway*		
GetHypervisor	Concede permissão para GetHypervisor	Leitura	hypervisor*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetHypervisorPropertyMappings	Concede permissão para GetHypervisorPropertyMappings	Leitura	hypervisor*		
GetVirtualMachine	Concede permissão para GetVirtualMachine	Leitura	virtualmachine*		
ImportHypervisorConfiguration	Concede permissão para ImportHypervisorConfiguration	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
ListGateways	Concede permissão para ListGateways	Leitura			
ListHypervisors	Concede permissão para ListHypervisors	Leitura			
ListTagsForResource	Concede permissão para ListTagsForResource	Leitura	gateway		
			hypervisor		
			virtualmachine		
ListVirtualMachines	Concede permissão para ListVirtualMachines	Leitura			
PutBandwidthRateLimitSchedule	Concede permissão para PutBandwidthRateLimitSchedule	Gravar	gateway*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutHypervisorPropertyMappings	Concede permissão para PutHypervisorPropertyMappings	Gravar	hypervisor*		iam:PassRole
PutMaintenanceStartTime	Concede permissão para PutMaintenanceStartTime	Gravar	gateway*		
Restore	Concede permissão para Restore	Gravar	hypervisor*		
StartVirtualMachinesMetadataSync	Concede permissão para StartVirtualMachinesMetadataSync	Gravar	hypervisor*		iam:PassRole
TagResource	Concede permissão para TagResource	Tags	gateway		
			hypervisor		
			virtualmachine		
				aws:RequestTag/${TagKey} aws:TagKeys	
TestHypervisorConfiguration	Concede permissão para TestHypervisorConfiguration	Gravar	gateway*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para UntagResource	Tags	gateway		
			hypervisor		
			virtualmachine		
				aws:TagKeys	
UpdateGatewayInformation	Concede permissão para UpdateGatewayInformation	Gravar	gateway*		
UpdateGatewaySoftwareNow	Concede permissão para UpdateGatewaySoftwareNow	Gravar	gateway*		
UpdateHypervisor	Concede permissão para UpdateHypervisor	Gravar	gateway*		

Tipos de recursos definidos pelo AWS Backup Gateway

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS Backup Gateway

AWS O Backup Gateway define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelo conjunto de valores permitido para cada uma das etiquetas	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelo valor-etiqueta associado ao recurso	String
aws:TagKeys	Filtra o acesso pela presença de etiquetas obrigatórias na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS Backup Search

AWS O Backup Search (prefixo do serviço:`backup-search`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Pesquisa AWS de Backup
- Tipos de recursos definidos pelo AWS Backup Search
- Chaves de condição para AWS Backup Search

Ações definidas pela Pesquisa AWS de Backup

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSearchJob	Concede permissão para obter detalhes de um trabalho de busca	Leitura	searchJob*		
GetSearchResultExportJob	Concede permissão para obter detalhes de um trabalho de exportação de resultados de pesquisa	Leitura	searchExportJob*		
ListSearchJobBackups	Concede permissão para listar backups no escopo de um trabalho de pesquisa	Leitura	searchJob*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListSearchJobResults	Concede permissão para listar os resultados de um trabalho de pesquisa	Leitura	searchJob*		
ListSearchJobs	Concede permissão para listar trabalhos de pesquisa	Lista			
ListSearchResultExportJobs	Concede permissão para listar trabalhos de exportação de resultados de pesquisa	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	searchExportJob		
			searchJob		
StartSearchJob	Concede permissão para criar um trabalho de busca	Gravar		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
StartSearchResultExportJob	Concede permissão para iniciar um trabalho de exportação para um trabalho de pesquisa existente	Gravar	searchJob*		iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
StopSearchJob	Concede permissão para interromper um trabalho de pesquisa em andamento	Gravar	searchJob*		
TagResource	Concede permissão para marcar um recurso	Marcação	searchExportJob		
			searchJob		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso	Tags	searchExportJob		
			searchJob		
				aws:TagKeys	

Tipos de recursos definidos pelo AWS Backup Search

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição para AWS Backup Search

AWS O Backup Search define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelo conjunto de valores permitido para cada uma das etiquetas	String

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra o acesso pela presença de etiquetas obrigatórias na solicitação	ArrayOfString

Ações, recursos e chaves de condição do armazenamento do armazenamento do AWS Backup

AWS O armazenamento de backup (prefixo do serviço:`backup-storage`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo armazenamento do AWS Backup
- Tipos de recursos definidos pelo armazenamento do AWS Backup
- Chaves de condição do armazenamento do AWS Backup

Ações definidas pelo armazenamento do AWS Backup

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CommitBackupJob [somente permissão]	Concede permissão para confirmar trabalho de backup	Gravar			
DeleteObjects [somente permissão]	Concede permissão para excluir objetos	Gravar			
DescribeBackupJob [somente permissão]	Concede permissão para descrever um trabalho de backup	Gravar			
GetBaseBackup [somente permissão]	Concede permissão para obter um backup básico	Gravar			
GetChunk [somente permissão]	Concede permissão para obter dados de um ponto de recuperação para um trabalho de restauração	Gravar			
GetIncrementalBaseBackup [somente permissão]	Concede permissão para obter um backup básico incremental	Gravar			
GetObjectMetadata	Concede permissão para obter metadados de um ponto	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
[somente permissão]	de recuperação para um trabalho de restauração				
ListChunks [somente permissão]	Concede permissão para listar dados de um ponto de recuperação para um trabalho de restauração	Gravar			
ListObjects [somente permissão]	Concede permissão para listar dados de um ponto de recuperação para um trabalho de restauração	Gravar			
MountCapsule [somente permissão]	Associa uma chave do KMS a um cofre de backup	Gravar			
NotifyObjectComplete [somente permissão]	Concede permissão para marcar um dado carregado como concluído para um trabalho de backup	Gravar			
PutChunk [somente permissão]	Concede permissão para carregar dados em um ponto de recuperação AWS gerenciado por backup para uma tarefa de backup	Gravar			
PutObject [somente permissão]	Concede permissão para colocar um objeto	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartObject [somente permissão]	Concede permissão para carregar dados em um ponto de recuperação AWS gerenciado por backup para uma tarefa de backup	Gravar			
UpdateObjectComplete [somente permissão]	Concede permissão para concluir a atualização de um objeto	Gravar			

Tipos de recursos definidos pelo armazenamento do AWS Backup

AWS O armazenamento de backup não suporta a especificação de um ARN de recurso no elemento de uma `Resource` declaração de política do IAM. Para conceder acesso ao armazenamento do AWS Backup, especifique `"Resource": "*"` na política.

Chaves de condição do armazenamento do AWS Backup

O armazenamento de backup não tem chaves de contexto específicas do serviço que podem ser usadas no elemento `Condition` das instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Batch

AWS O Batch (prefixo do serviço:`batch`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.

- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Batch
- Tipos de recursos definidos pelo AWS Batch
- Chaves de condição do AWS Batch

Ações definidas pelo AWS Batch

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelJob	Concede permissão para cancelar um trabalho em uma fila de trabalhos do AWS Batch em sua conta	Gravar	job*		
CreateComputeEnvironment	Concede permissão para criar um ambiente de computação AWS Batch em sua conta	Gravar	compute-environment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConsumableResource	Concede permissão para criar um recurso consumível AWS Batch em sua conta	Gravar	consumable-resource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateJobQueue	Concede permissão para criar uma fila AWS de trabalhos do Batch em sua conta	Gravar	job-queue*	aws:RequestTag/${TagKey} aws:TagKeys	
			compute-environment		
			scheduling-policy		
			service-environment		
CreateSchedulingPolicy	Concede permissão para criar uma política de agendamento de AWS Batch em sua conta	Gravar	scheduling-policy*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateServiceEnvironment	Concede permissão para criar um ambiente de serviço AWS Batch em sua conta	Gravar	service-environment*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteComputeEnvironment	Concede permissão para excluir um ambiente de computação AWS Batch em sua conta	Gravar	compute-environment*		
DeleteConsumableResource	Concede permissão para excluir um recurso consumível do AWS Batch em sua conta	Gravar	consumable-resource*		
DeleteJobQueue	Concede permissão para excluir uma fila AWS de trabalhos do Batch em sua conta	Gravar	job-queue*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteSchedulingPolicy	Concede permissão para excluir uma política de agendamento de AWS Batch em sua conta	Gravar	scheduling-policy*		
DeleteServiceEnvironment	Concede permissão para excluir um ambiente de serviço AWS Batch em sua conta	Gravar	service-environment*		
DeregisterJobDefinition	Concede permissão para cancelar o registro de uma definição de tarefa do AWS Batch em sua conta	Gravar	job-definition-revision*		
DescribeComputeEnvironments	Concede permissão para descrever um ou mais ambientes de computação AWS Batch em sua conta	Leitura			
DescribeConsumableResource	Concede permissão para descrever um ou mais recursos consumíveis do AWS Batch em sua conta	Leitura	consumable-resource*		
DescribeJobDefinitions	Concede permissão para descrever uma ou mais definições de trabalho do AWS Batch em sua conta	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeJobQueues	Concede permissão para descrever uma ou mais filas de trabalhos do AWS Batch em sua conta	Leitura			
DescribeJobs	Concede permissão para descrever uma lista de trabalhos em AWS Batch em sua conta	Leitura			
DescribeSchedulingPolicies	Concede permissão para descrever uma ou mais políticas de agendamento de AWS Batch em sua conta	Leitura			
DescribeServiceEnvironments	Concede permissão para descrever um ou mais ambientes de serviço AWS Batch em sua conta	Leitura			
DescribeServiceJob	Concede permissão para descrever um trabalho do serviço AWS Batch em sua conta	Leitura			
GetJobQueueSnapshot	Concede permissão para obter um instantâneo de uma fila de trabalhos do AWS Batch em sua conta	Leitura	job-queue*		
ListConsumableResources	Concede permissão para listar recursos consumíveis do AWS Batch em sua conta	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListJobs	Concede permissão para listar trabalhos para uma fila de trabalhos do AWS Batch especificada em sua conta	Lista			
ListJobsByConsumableResource	Concede permissão para listar trabalhos AWS em Batch que exigem um recurso consumível específico em sua conta	Lista	consumable-resource*		
ListSchedulingPolicies	Concede permissão para listar políticas AWS de agendamento de Batch em sua conta	Leitura			
ListServiceJobs	Concede permissão para listar trabalhos de serviço para uma fila de trabalhos do AWS Batch especificada em sua conta	Lista			
ListTagsForResource	Concede permissão para listar tags para um recurso do AWS Batch em sua conta	Leitura	compute-environment		
			consumable-resource		
			job		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			job-definition-revision		
			job-queue		
			scheduling-policy		
			service-environment		
			service-job		
RegisterJobDefinition	Concede permissão para registrar uma definição AWS de tarefa do Batch em sua conta	Gravar	job-definition*		
			consumable-resource		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				batch:User batch:Privileged batch:Image batch:LogDriver batch:AWSLogsGroup batch:AWSLogsRegion batch:AWSLogsStreamPrefix batch:AWSLogsCreateGroup batch:EKSServiceAccountName batch:EKSImage	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				batch:EKSRunAsUser batch:EKSRunAsGroup batch:EKSPrivileged batch:EKSNamespace aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SubmitJob	Concede permissão para enviar um trabalho AWS em Batch a partir de uma definição de trabalho em sua conta	Gravar	job*	batch:ShareIdentifier batch:EKSImage batch:EKSNamespace aws:RequestTag/${TagKey} aws:TagKeys	
			job-definition*		
			job-queue*		
			consumable-resource		
SubmitServiceJob	Concede permissão para enviar um trabalho de serviço do AWS Batch	Gravar	job-queue*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			service-job*	batch:ShareIdentifier aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Concede permissão para marcar um recurso do AWS Batch em sua conta	Tags	compute-environment		
			consumable-resource		
			job		
			job-definition-revision		
			job-queue		
			scheduling-policy		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			service-environment		
			service-job		
				aws:RequestTag/${TagKey} aws:TagKeys	
TerminateJob	Concede permissão para encerrar um trabalho em uma fila de trabalhos do AWS Batch em sua conta	Gravar	job*		
TerminateServiceJob	Concede permissão para encerrar um trabalho de serviço em uma fila de trabalhos do AWS Batch em sua conta	Gravar	service-job*		
UntagResource	Concede permissão para desmarcar um recurso do AWS Batch em sua conta	Tags	compute-environment		
			consumable-resource		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			job		
			job-definition-revision		
			job-queue		
			scheduling-policy		
			service-environment		
			service-job		
				aws:TagKeys	
UpdateComputeEnvironment	Concede permissão para atualizar um ambiente de computação AWS Batch em sua conta	Gravar	compute-environment*		
UpdateConsumableResource	Concede permissão para atualizar um recurso consumível do AWS Batch em sua conta	Gravar	consumable-resource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateJobQueue	Concede permissão para atualizar uma fila AWS de trabalhos do Batch em sua conta	Gravar	job-queue*		
			compute-environment		
			scheduling-policy		
UpdateSchedulingPolicy	Concede permissão para atualizar uma política de agendamento de AWS Batch em sua conta	Gravar	scheduling-policy*		
UpdateServiceEnvironment	Concede permissão para atualizar um ambiente de serviço AWS Batch em sua conta	Gravar	service-environment*		

Tipos de recursos definidos pelo AWS Batch

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
compute-environment	arn:${Partition}:batch:${Region}:${Account}:compute-environment/${ComputeEnvironmentName}	aws:ResourceTag/${TagKey}
job-queue	arn:${Partition}:batch:${Region}:${Account}:job-queue/${JobQueueName}	aws:ResourceTag/${TagKey}
job-definition	arn:${Partition}:batch:${Region}:${Account}:job-definition/${JobDefinitionName}	
job-definition-revision	arn:${Partition}:batch:${Region}:${Account}:job-definition/${JobDefinitionName}:${Revision}	aws:ResourceTag/${TagKey}
job	arn:${Partition}:batch:${Region}:${Account}:job/${JobId}	aws:ResourceTag/${TagKey}
scheduling-policy	arn:${Partition}:batch:${Region}:${Account}:scheduling-policy/${SchedulingPolicyName}	aws:ResourceTag/${TagKey}
service-environment	arn:${Partition}:batch:${Region}:${Account}:service-environment/${ServiceEnvironmentName}	aws:ResourceTag/${TagKey}
service-job	arn:${Partition}:batch:${Region}:${Account}:service-job/${JobId}	aws:ResourceTag/${TagKey}
consumable-resource	arn:${Partition}:batch:${Region}:${Account}:consumable-resource/${ConsumableResourceName}	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Batch

AWS O Batch define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString
batch:AWSLogsCreateGroup	Filtra o acesso pelo driver de log especificado para determinar se o grupo do awslogs será criado para os logs	Bool
batch:AWSLogsGroup	Filtra o acesso pelo grupo do awslogs em que os logs estão localizados	String
batch:AWSLogsRegion	Filtra o acesso pela região para a qual os logs são enviados	String
batch:AWSLogsStreamPrefix	Filtra o acesso pelo prefixo do fluxo do log do awslogs	String
batch:EKSImage	Filtra o acesso pela imagem usada para iniciar um contêiner para um trabalho do Amazon EKS	String

Chaves de condição	Descrição	Tipo
batch:EKSNamespace	Filtra o acesso pelo namespace de um cluster usado para executar o pod para uma tarefa do Amazon EKS	String
batch:EKSPrivileged	Filtra o acesso pelo valor de parâmetro privilegiado especificado que determina se o contêiner recebe privilégios elevados na instância de contêiner de host (semelhante ao usuário raiz) para um trabalho do Amazon EKS	Bool
batch:EKSRunAsGroup	Filtra o acesso pelo ID numérico do grupo especificado (gid) usado para iniciar um contêiner em um trabalho do Amazon EKS	Numérico
batch:EKSRunAsUser	Filtra o acesso pelo ID numérico do grupo especificado (uid) usado para iniciar um contêiner em um trabalho do Amazon EKS	Numérico
batch:EKSServiceAccountName	Filtra o acesso pelo nome da conta de serviço usada para executar o pod para um trabalho do Amazon EKS	String
batch:Image	Filtra o acesso pela imagem usada para iniciar um contêiner	String
batch:LogDriver	Filtra o acesso pelo driver de log usado para o contêiner	String
batch:Privileged	Filtra o acesso pelo valor de parâmetro privilegiado especificado que determina se o contêiner recebe privilégios elevados na instância de contêiner host (semelhante ao usuário raiz)	Bool
batch:ShareIdentifier	Filtra o acesso pelo ShareIdentifier usado dentro do trabalho de envio	String
batch:User	Filtra o acesso pelo nome de usuário ou uid numérico usado dentro do contêiner	String

Ações, recursos e chaves de condição do Amazon Bedrock

O Amazon Bedrock (prefixo do serviço: `bedrock`) fornece os recursos, ações e chaves de contexto de condição a seguir, específicos do serviço, para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Bedrock
- Tipos de recursos definidos pelo Amazon Bedrock
- Chaves de condição do Amazon Bedrock

Ações definidas pelo Amazon Bedrock

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AllowVendedLogDeliveryForResource [somente permissão]	Concede permissão para configurar a entrega de logs fornecidos para uma base de conhecimento	Gerenciamento de permissões	knowledge-base		
ApplyGuardrail	Concede permissão para aplicar uma barreira de proteção	Leitura	guardrail*		
			guardrail-profile		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateAgentCollaborator	Concede permissão para associar outro agente existente como colaborador a um agente existente	Gravar	agent*		
AssociateAgentKnowledgeBase	Concede permissão para associar uma base de conhecimento a um agente	Gravar	agent*		
			knowledge-base*		
AssociateThirdPartyKnowledgeBase [somente permissão]	Concede permissão para usar uma plataforma de terceiros para armazenar dados de conhecimento	Gravar		bedrock:ThirdPartyKnowledgeBaseCredentialsSecretArn	
BatchDeleteEvaluationJob	Concede permissão para excluir em lote uma lista de trabalhos de avaliação do Bedrock	Gravar	evaluation-job*		
CallWithBearerToken	Concede permissão para usar o token do portador	Leitura			
CancelAutomatedReasoningPolicyBuildWorkflow	Concede permissão para cancelar um fluxo de trabalho de criação para uma política de raciocínio automatizado	Gravar	automated-reasoning-policy*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAgent	Concede permissão para criar um novo agente e um alias de agente de teste apontando para a versão DRAFT do agente	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAgentActionGroup	Concede permissão para criar um novo grupo de ação em um agente existente	Gravar	agent*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAgentAlias	Concede permissão para criar uma novo alias para um agente	Gravar	agent*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAutomatedReasoningPolicy	Concede permissão para criar uma nova política de raciocínio automatizado	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAutomatedReasoningPolicyTestCase	Concede permissão para criar um caso de teste para uma política de raciocínio automatizado	Gravar	automated-reasoning-policy*		
CreateAutomatedReasoningPolicyVersion	Concede permissão para criar uma nova versão da política de raciocínio automatizado	Gravar	automated-reasoning-policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBlueprint	Concede permissão para criar um plano para saída personalizada da automação de dados	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateBlueprintVersion	Concede permissão para criar uma nova versão para um blueprint existente	Gravar	blueprint*		
CreateCustomModel	Concede permissão para criar um modelo personalizado no Bedrock	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateCustomModelDeployment	Concede permissão para criar uma implantação de modelo personalizado para modelo personalizado	Gravar	custom-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataAutomationProject	Concede permissão para criar um projeto de automação de dados	Gravar	blueprint		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSource	Concede permissão para criar uma fonte de dados	Gravar	knowledge-base*		
CreateEvaluationJob	Concede permissão para criar um trabalho para modelos de base de avaliação ou modelos personalizados	Gravar	custom-model*		
			default-prompt-router*		
			foundation-model*		
			prompt-router*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFlow	Concede permissão para criar um fluxo de prompts	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFlowAlias	Concede permissão para criar um alias de um fluxo de prompt	Gravar	flow*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFlowVersion	Concede permissão para criar uma versão imutável de um fluxo de prompt	Gravar	flow*		
CreateFoundationModelAgreement	Concede permissão para criar um novo acordo de modelo de base	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateGuardrail	Concede permissão para criar uma nova barreira de proteção	Gravar	automated-reasoning-policy		
			automated-reasoning-policy-version		
			guardrail-profile		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateGuardrailVersion	Concede permissão para criar uma nova versão da barreira de proteção	Gravar	guardrail*		
CreateInferenceProfile	Concede permissão para criar perfis de inferência	Gravar	application-inference-profile*		
			foundation-model*		
			inference-profile*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInvocation	Concede permissão para criar uma nova invocação em uma sessão existente	Gravar	session*		
CreateKnowledgeBase	Concede permissão para criar uma base de conhecimentos	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateMarketplaceModelEndpoint	Concede permissão para criar um endpoint de modelo de mercado	Gravar			
CreateModelCopyJob	Concede permissão para criar um trabalho e copiar um modelo personalizado em várias regiões ou contas	Gravar	custom-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateModelCustomizationJob	Concede permissão para criar um trabalho para personalizar o modelo com seus dados de treinamento personalizados	Gravar	custom-model*		
			foundation-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelEvaluationJob	Concede permissão para criar um trabalho para modelos de base de avaliação ou modelos personalizados	Gravar	custom-model*		
			foundation-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelImportJob	Concede permissão para criar um trabalho e importar um modelo no Bedrock	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateModelInvocationJob	Concede permissão para criar um trabalho de invocação de modelo	Gravar	custom-model*		
			foundation-model*		
			model-invocation-job*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePrompt	Concede permissão para criar um prompt	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePromptRouter	Concede permissão para criar um roteador de prompt personalizado	Gravar	application-inference-profile*		
			foundation-model*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			inference-profile*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePromptVersion	Concede permissão para criar uma versão de um prompt	Gravar	prompt*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProvisionedModelThroughput	Concede permissão para criar uma nova throughput de modelo provisionado	Gravar	custom-model*		
			foundation-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSession	Concede permissão para criar uma nova sessão	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAgent	Concede permissão para excluir um agente criado anteriormente	Gravar	agent*		
DeleteAgentActionGroup	Concede permissão para excluir um actionGroup criado anteriormente	Gravar	agent*		
DeleteAgentAlias	Concede permissão para excluir um AgentAlias que você criou anteriormente	Gravar	agent-alias*		
DeleteAgentMemory	Concede permissão para excluir a memória existente de um alias	Gravar	agent-alias*		
DeleteAgentVersion	Concede permissão para excluir uma versão de agente criado anteriormente	Gravar	agent*		
DeleteAutomatedReasoningPolicy	Concede permissão para excluir uma política de raciocínio automatizado ou sua versão	Gravar	automated-reasoning-policy*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			automated-reasoning-policy-version*		
DeleteAutomatedReasoningPolicyBuildWorkflow	Concede permissão para excluir um fluxo de trabalho de criação para uma política de raciocínio automatizado	Gravar	automated-reasoning-policy*		
DeleteAutomatedReasoningPolicyTestCase	Concede permissão para excluir um caso de teste para uma política de raciocínio automatizado	Gravar	automated-reasoning-policy*		
DeleteBlueprint	Concede permissão para excluir um plano para automação de dados	Gravar	blueprint*		
DeleteCustomModel	Concede permissão para excluir um modelo personalizado que você criou anteriormente	Gravar	custom-model*		
DeleteCustomModelDeployment	Concede permissão para excluir uma implantação de modelo personalizado que você criou anteriormente	Gravar	custom-model-deployment*		
DeleteDataAutomationProject	Concede permissão para excluir um projeto de automação de dados	Gravar	data-automation-project*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteDataSource	Concede permissão para excluir uma fonte de dados	Gravar	knowledge-base*		
DeleteFlow	Concede permissão para excluir um fluxo de prompts	Gravar	flow*		
DeleteFlowAlias	Concede permissão para excluir um alias de um fluxo de prompt	Gravar	flow-alias*		
DeleteFlowVersion	Concede permissão para excluir uma versão de um fluxo de prompts	Gravar	flow*		
DeleteFoundationModelAgreement	Concede permissão para excluir um contrato de modelo de base que você criou anteriormente	Gravar			
DeleteGuardrail	Concede permissão para criar uma barreira de proteção ou sua versão	Gravar	guardrail*		
DeleteImportedModel	Concede permissão para excluir um modelo importado do Bedrock criado anteriormente	Gravar	imported-model*		
DeleteInferenceProfile	Concede permissão para excluir perfis de inferência	Gravar	application-inference-profile*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteKnowledgeBase	Concede permissão para excluir uma base de conhecimentos	Gravar	knowledge-base*		
DeleteKnowledgeBaseDocuments	Concede permissão para excluir documentos de uma base de conhecimento	Gravar	knowledge-base*		
DeleteMarketplaceModelAgreement	Concede permissão para cancelar a assinatura de um modelo de mercado baseado em um mercado básico AWS	Gravar			
DeleteMarketplaceModelEndpoint	Concede permissão para excluir um endpoint do modelo de mercado	Gravar	bedrock-marketplace-model-endpoint*		
DeleteModelInvocationLoggingConfiguration	Concede permissão para excluir uma configuração de registro em log de invocação existente	Gravar			
DeletePrompt	Concede permissão para excluir um prompt ou sua versão	Gravar	prompt*		
			prompt-version*		
DeletePromptRouter	Concede permissão para excluir um roteador de prompt personalizado	Gravar	prompt-router*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteProvisionedModelThroughput	Concede permissão para excluir um throughput de modelo provisionado que você criou anteriormente	Gravar	provisioned-model*		
DeleteResourcePolicy [somente permissão]	Exclui uma política de recursos do Bedrock criada anteriormente	Gravar	custom-model*		
DeleteSession	Concede permissão para excluir uma sessão que você criou anteriormente	Gravar	session*		
DeregisterMarketplaceModelEndpoint	Concede permissão para cancelar o registro de um endpoint do modelo de mercado para torná-lo inutilizável no Bedrock Marketplace	Gravar	bedrock-marketplace-model-endpoint*		
DetectGeneratedContent	Concede permissão para detectar se o conteúdo fornecido é gerado usando o Amazon Bedrock	Leitura	foundation-model*		
DisassociateAgentCollaborator	Concede permissão para desassociar um colaborador que você associou anteriormente	Gravar	agent*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateAgentKnowledgeBase	Concede permissão para desassociar uma base de conhecimento do agente	Gravar	agent*		
			knowledge-base*		
EndSession	Concede permissão para encerrar uma sessão que você criou anteriormente	Gravar	session*		
ExportAutomatedReasoningPolicyVersion	Concede permissão para recuperar um artefato automatizado da versão da política de raciocínio	Leitura	automated-reasoning-policy*		
			automated-reasoning-policy-version*		
GenerateQuery	Concede permissão para gerar consultas associadas à entrada do usuário	Leitura			
GetAgent	Concede permissão para recuperar um agente existente	Leitura	agent*		
GetAgentActionGroup	Concede permissão para recuperar um grupo de ação existente	Leitura	agent*		
GetAgentAlias	Concede permissão para recuperar um alias existente	Leitura	agent-alias*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAgentCollaborator	Concede permissão para recuperar um colaborador existente	Leitura	agent*		
GetAgentKnowledgeBase	Concede permissão para descrever uma base de conhecimento associada a um agente	Leitura	agent*		
			knowledge-base*		
GetAgentMemory	Concede permissão para recuperar memória existente de um alias	Leitura	agent-alias*		
GetAgentVersion	Concede permissão para recuperar uma versão existente de um agente	Leitura	agent*		
GetAsyncInvoke	Concede permissão para obter as propriedades associadas a uma invocação assíncrona que você enviou	Leitura	async-invoke*		
GetAutomatedReasoningPolicy	Concede permissão para recuperar uma política de raciocínio automatizado ou sua versão	Leitura	automated-reasoning-policy*		
			automated-reasoning-policy-version*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAutomatedReasoningPolicyAnnotations	Concede permissão para recuperar anotações para um fluxo de trabalho de criação para uma política de raciocínio automatizada	Leitura	automated-reasoning-policy*		
GetAutomatedReasoningPolicyBuildWorkflow	Concede permissão para recuperar um fluxo de trabalho de criação para uma política de raciocínio automatizada	Leitura	automated-reasoning-policy*		
GetAutomatedReasoningPolicyBuildWorkflowResultAssets	Concede permissão para recuperar ativos para um fluxo de trabalho de criação para uma política de raciocínio automatizada	Leitura	automated-reasoning-policy*		
GetAutomatedReasoningPolicyNextScenario	Concede permissão para recuperar o próximo cenário gerado não revisado para um fluxo de trabalho de criação de uma política de raciocínio automatizada	Leitura	automated-reasoning-policy*		
GetAutomatedReasoningPolicyTestCase	Concede permissão para recuperar um caso de teste para uma política de raciocínio automatizado	Leitura	automated-reasoning-policy*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAutomatedReasoningPolicyTestResult	Concede permissão para recuperar o resultado de um caso de teste para uma política de raciocínio automatizado	Leitura	automated-reasoning-policy*		
GetBlueprint	Concede permissão para recuperar um plano existente para automação de dados	Leitura	blueprint*		
GetBlueprintRecommendation [somente permissão]	Concede permissão para recuperar a recomendação do plano	Leitura			
GetCustomModel	Concede permissão para obter as propriedades associadas a um modelo personalizado Bedrock que você criou	Leitura	custom-model*		
GetCustomModelDeployment	Concede permissão para obter as propriedades associadas à implantação de um modelo personalizado. Use essa operação para obter o status de uma implantação de modelo personalizado	Leitura	custom-model-deployment*		
GetDataAutomationProject	Concede permissão para recuperar um projeto de automação de dados existente	Leitura	data-automation-project*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetDataAutomationStatus	Concede permissão para recuperar o status de um trabalho de invocação de automação de dados	Leitura	data-automation-invocation-job*		
GetDataSource	Concede permissão para recuperar uma fonte de dados existente	Leitura	knowledge-base*		
GetEvaluationJob	Concede permissão para obter as propriedades associadas a um trabalho de avaliação. Use essa operação para obter o status de um trabalho de avaliação	Leitura	evaluation-job*		
GetExecutionFlowSnapshot	Concede permissão para recuperar a definição de fluxo para uma execução de fluxo	Leitura	flow*		
			flow-alias*		
			flow-execution*		
GetFlow	Concede permissão para recuperar um fluxo de prompt existente	Leitura	flow*		
GetFlowAlias	Concede permissão para recuperar um alias existente de um fluxo de prompts	Leitura	flow-alias*		
GetFlowExecution		Leitura	flow*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	Concede permissão para recuperar uma execução existente de um alias de fluxo		flow-alias*		
			flow-execution*		
GetFlowVersion	Concede permissão para recuperar uma versão existente de um fluxo de prompt	Leitura	flow*		
GetFoundationModel	Concede permissão para obter as propriedades associadas a um modelo de base do Bedrock	Leitura	foundation-model*		
GetFoundationModelAvailability	Concede permissão para obter a disponibilidade de um modelo de base	Leitura			
GetGuardrail	Concede permissão para recuperar uma barreira de proteção ou sua versão	Leitura	guardrail*		
GetImportedModel	Concede permissão para obter as propriedades associadas ao modelo importado do Bedrock	Leitura	imported-model*		
GetInferenceProfile	Concede permissão para obter as propriedades associadas a um perfil de inferência	Leitura	application-inference-profile*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			inference-profile*		
GetIngestionJob	Concede permissão para recuperar um trabalho de ingestão existente	Leitura	knowledge-base*		
GetInvocationStep	Concede permissão para obter uma etapa de invocação de uma sessão	Leitura	session*		
GetKnowledgeBase	Concede permissão para recuperar uma base de conhecimento existente	Leitura	knowledge-base*		
GetKnowledgeBaseDocuments	Concede permissão para obter detalhes de documentos em uma base de conhecimento	Leitura	knowledge-base*		
GetMarketplaceModelEndpoint	Concede permissão para obter as propriedades de um endpoint do modelo de mercado	Leitura	bedrock-marketplace-model-endpoint*		
GetModelCopyJob	Concede permissão para obter as propriedades associadas a um trabalho de cópia de modelo. Use essa operação para obter o status de um trabalho de cópia de modelo	Leitura	model-copy-job*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetModelCustomizationJob	Concede permissão para obter as propriedades associadas a um trabalho de personalização de modelo. Use essa operação para obter o status de uma tarefa de personalização do modelo	Leitura	model-customization-job*		
GetModelEvaluationJob	Concede permissão para obter as propriedades associadas a um trabalho de avaliação de modelo. Use essa operação para obter o status de um trabalho de avaliação de modelo	Leitura	model-evaluation-job*		
GetModelImportJob	Concede permissão para obter as propriedades associadas a um trabalho de importação de modelos, sendo usada para obter o status de um trabalho de importação de modelos	Leitura	model-import-job*		
GetModelInvocationJob	Concede permissão para recuperar um trabalho de invocação de modelo	Leitura	model-invocation-job*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetModelInvocationLoggingConfiguration	Concede permissão para recuperar uma configuração de registro em log de invocação existente	Leitura			
GetPrompt	Concede permissão para recuperar um prompt existente ou sua versão	Leitura	prompt*		
			prompt-version*		
GetPromptRouter	Concede permissão para obter as propriedades associadas a um roteador de prompt		default-prompt-router*		
			prompt-router*		
GetProvisionedModelThroughput	Concede permissão para recuperar uma throughput de modelo provisionado	Leitura	provisioned-model*		
GetResourcePolicy [somente permissão]	Obtém o documento da política de recursos para um recurso do Bedrock	Leitura	custom-model*		
GetSession	Concede permissão para recuperar uma sessão existente	Leitura	session*		
GetUseCaseForModelAccess	Concede permissão para recuperar um caso de uso para acesso ao modelo	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
IngestKnowledgeBaseDocuments	Concede permissão para ingerir documentos diretamente em uma base de conhecimento	Gravar	knowledge-base*		
InvokeAgent	Concede permissão para enviar a colaboração do usuário (somente em texto) para o alias de um agente para o Bedrock	Leitura	agent-alias*		
InvokeAutomatedReasoningPolicy [somente permissão]	Concede permissão para invocar uma política de raciocínio automatizado	Leitura	automated-reasoning-policy*		
			automated-reasoning-policy-version*		
InvokeBlueprintRecommendationAsync [somente permissão]	Concede permissão para invocar recomendações de blueprint de forma assíncrona	Gravar	data-automation-profile*		
InvokeBuilder [somente permissão]	Concede permissão para usar o construtor de conversação, que ajuda na criação de recursos compatíveis do Bedrock	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
InvokeDataAutomationAsync	Concede permissão para invocar um trabalho de automação de dados da Bedrock	Gravar	blueprint*		
			data-automation-profile*		
			data-automation-project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
InvokeFlow	Concede permissão para invocar um fluxo de prompt com a entrada do usuário	Leitura	flow-alias*		
InvokeInlineAgent	Concede permissão para enviar a entrada do usuário (somente texto) para o agente embutido do Bedrock	Leitura		bedrock:InlineAgentName	
InvokeModel	Concede permissão para invocar o modelo Bedrock especificado para executar a inferência usando a entrada fornecida no corpo da solicitação	Leitura	application-inference-profile*		
			async-invoke*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			bedrock-marketplace-model-endpoint*		
			custom-model-deployment*		
			default-prompt-router*		
			foundation-model*		
			imported-model*		
			inference-profile*		
			prompt-router*		
			provisioned-model*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				bedrock:InferenceProfileArn bedrock:PromptRouterArn aws:RequestTag/${TagKey} aws:TagKeys bedrock:GuardrailIdentifier	
InvokeModelWithResponseStream	Concede permissão para invocar o modelo Bedrock especificado para executar a inferência usando a entrada fornecida no corpo da solicitação com resposta de streaming	Leitura	application-inference-profile*		
			bedrock-marketplace-model-endpoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			custom-model-deployment*		
			default-prompt-router*		
			foundation-model*		
			imported-model*		
			inference-profile*		
			prompt-router*		
			provisioned-model*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				bedrock:InferenceProfileArn bedrock:PromptRouterArn bedrock:GuardrailIdentifier	
ListAgentActionGroups	Concede permissão para listar grupos de ação em um agente	Lista	agent*		
ListAgentAliases	Concede permissão para listar os aliases de um agente	Lista	agent*		
ListAgentCollaborators	Concede permissão para listar colaboradores para um agente	Lista	agent*		
ListAgentKnowledgeBases	Concede permissão para listar bases de conhecimento associadas a um agente	Lista	agent*		
ListAgentVersions	Concede permissão para listar versões existentes de um agente	Lista	agent*		
ListAgents	Concede permissão para listar os agentes existentes	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAsyncInvokes	Concede permissão para obter uma lista de invocações assíncronas que você enviou	Lista			
ListAutomatedReasoningPolicies	Concede permissão para listar políticas de raciocínio automatizado ou suas versões	Lista	automated-reasoning-policy		
ListAutomatedReasoningPolicyBuildWorkflows	Concede permissão para criar fluxos de trabalho de lista para uma política de raciocínio automatizada	Lista	automated-reasoning-policy*		
ListAutomatedReasoningPolicyTestCases	Concede permissão para listar casos de teste para uma política de raciocínio automatizado	Lista	automated-reasoning-policy*		
ListAutomatedReasoningPolicyTestResults	Concede permissão para listar o resultado do teste para uma política de raciocínio automatizado	Lista	automated-reasoning-policy*		
ListBlueprints	Concede permissão para listar esquemas existentes para automação de dados	Lista	data-automation-project		
ListCustomModelDeployments	Concede permissão para obter a lista de implantações de modelos personalizados que você enviou	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListCustomModels	Concede permissão para obter uma lista de modelos personalizados Bedrock que você criou	Lista			
ListDataAutomationProjects	Concede permissão para listar projetos de automação de dados existentes	Lista	blueprint		
ListDataSources	Concede permissão para listar fontes de dados existentes em uma base de conhecimento	Lista	knowledge-base*		
ListEvaluationJobs	Concede permissão para obter a lista de trabalhos de avaliação que você enviou	Lista			
ListFlowAliases	Concede permissão para listar alias existentes de um fluxo de prompt	Lista	flow*		
ListFlowExecutionEvents	Concede permissão para recuperar eventos para a execução de um fluxo	Lista	flow*		
			flow-alias*		
			flow-execution*		
ListFlowExecutions	Concede permissão para listar as execuções de um fluxo ou de um alias de fluxo	Lista	flow*		
			flow-alias		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListFlowVersions	Concede permissão para listar versões existentes de um fluxo de prompts	Lista	flow*		
ListFlows	Concede permissão para listar fluxos de prompts existentes	Lista			
ListFoundationModelAgreementOffers	Concede permissão para obter uma lista de ofertas de acordo de modelos de base	Lista			
ListFoundationModels	Concede permissão para listar modelos da Bedrock Foundation que você pode usar	Lista			
ListGuardrails	Concede permissão para listar barreiras de proteção ou suas versões	Lista	guardrail		
ListImportedModels	Concede permissão para obter uma lista de modelos importados do Bedrock	Lista			
ListInferenceProfiles	Concede permissão para listar perfis de inferências que podem ser usados	Lista			
ListIngestionJobs	Concede permissão para listar trabalhos de ingestão em uma fonte de dados	Lista	knowledge-base*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListInvocationSteps	Concede permissão para obter a lista da etapa de invocação de uma sessão	Lista	session*		
ListInvocations	Concede permissão para listar invocações em uma sessão	Lista	session*		
ListKnowledgeBaseDocuments	Concede permissão para listar documentos em uma base de conhecimento	Lista	knowledge-base*		
ListKnowledgeBases	Concede permissão para listar bases de conhecimento existentes	Lista			
ListMarketplaceModelEndpoints	Concede permissão para listar endpoints do modelo de mercado que você pode usar	Leitura			
ListModelCopyJobs	Concede permissão para obter a lista de trabalhos de cópia de modelo que você enviou	Lista			
ListModelCustomizationJobs	Concede permissão para obter a lista de trabalhos de personalização de modelo que você enviou	Lista			
ListModelEvaluationJobs	Concede permissão para obter a lista de trabalhos de avaliação de modelo que você enviou	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListModelImportJobs	Concede permissão para obter uma lista de trabalhos de importação de modelos	Lista			
ListModelInvocationJobs	Concede permissão para listar trabalhos de invocação de modelos criados anteriormente	Lista			
ListPromptRouters	Concede permissão para listar roteadores de prompt que você pode usar	Lista			
ListPrompts	Concede permissão para listar prompts existentes	Lista	prompt		
ListProvisionedModelThroughputs	Concede permissão para listar throughputs de modelos provisionados que você criou anteriormente	Lista			
ListSessions	Concede permissão para listar sessões existentes	Lista			
ListTagsForResource	Concede permissão para listar as tags de um recurso Bedrock	Leitura	agent*		
			agent-alias*		
			application-inference-profile*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			async-invoke*		
			automated-reasoning-policy*		
			automated-reasoning-policy-version*		
			blueprint*		
			custom-model*		
			custom-model-deployment*		
			data-automation-invocation-job*		
			data-automation-project*		
			evaluation-job*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			flow*		
			flow-alias*		
			guardrail*		
			imported-model*		
			knowledge-base*		
			model-copy-job*		
			model-customization-job*		
			model-evaluation-job*		
			model-import-job*		
			model-invocation-job*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			prompt*		
			prompt-router*		
			prompt-version*		
			provisioned-model*		
			session*		
OptimizePrompt	Concede permissão para otimizar um prompt com a entrada do usuário	Leitura			
PrepareAgent	Concede permissão para preparar um agente existente para receber solicitações no runtime	Gravar	agent*		
PrepareFlow	Concede permissão para aplicar as alterações mais recentes feitas em um fluxo de prompt, para que elas sejam refletidas no runtime	Gravar	flow*		
PutFoundationModelEntitlement	Concede permissão para autorizar o acesso a um modelo de base	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutInvocationStep	Concede permissão para colocar uma etapa de invocação em uma invocação na sessão	Gravar	session*		
PutModelInvocationLoggingConfiguration	Concede permissão para criar uma configuração de registro em log de invocação existente	Gravar			
PutResourcePolicy [somente permissão]	Adiciona uma política de recurso para um recurso do Bedrock	Gravar	custom-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutUseCaseForModelAccess	Concede permissão para inserir um caso de uso para acesso ao modelo	Gravar			
RegisterMarketplaceModelEndpoint	Concede permissão para registrar um endpoint do Sagemaker como um endpoint do modelo de mercado	Gravar	bedrock-marketplace-model-endpoint*		
RenderPrompt [somente permissão]	Concede permissão para renderizar um prompt existente ou sua versão	Leitura	prompt*		
			prompt-version*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
Rerank	Concede permissão para classificar documentos com base na entrada do usuário	Gravar			
Retrieve	Concede permissão para recuperar dados ingeridos de uma base de conhecimento	Leitura	knowledge-base*		
RetrieveAndGenerate	Concede permissão para enviar a colaboração do usuário para realizar a recuperação e geração	Gravar			
StartAutomatedReasoningPolicyBuildWorkflow	Concede permissão para iniciar um fluxo de trabalho de criação para uma política de raciocínio automatizada	Gravar	automated-reasoning-policy*		
StartAutomatedReasoningPolicyTestWorkflow	Concede permissão para iniciar um fluxo de trabalho de teste para uma política de raciocínio automatizado	Gravar	automated-reasoning-policy*		
StartFlowExecution	Concede permissão para iniciar a execução de um alias de fluxo	Gravar	flow* flow-alias*		
StartIngestionJob	Concede permissão para iniciar um trabalho de ingestão	Gravar	knowledge-base*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopEvaluationJob	Concede permissão para interromper um trabalho de avaliação em andamento	Gravar	evaluation-job*		
StopFlowExecution	Concede permissão para interromper a execução de um alias de fluxo	Gravar	flow*		
			flow-alias*		
			flow-execution*		
StopIngestionJob	Concede permissão para interromper um trabalho de ingestão	Gravar	knowledge-base*		
StopModelCustomizationJob	Concede permissão para interromper um trabalho de personalização do modelo Bedrock enquanto estiver em andamento	Gravar	model-customization-job*		
StopModelInvocationJob	Concede permissão para interromper um trabalho de invocação de modelo iniciado anteriormente	Gravar	model-invocation-job*		
TagResource	Concede permissão para marcar um recurso Bedrock	Tags	agent		
			agent-alias		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			application-inference-profile		
			async-invoke		
			automated-reasoning-policy		
			automated-reasoning-policy-version		
			blueprint		
			custom-model		
			custom-model-deployment		
			data-automation-invocation-job		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			data-automation-project		
			evaluation-job		
			flow		
			flow-alias		
			guardrail		
			imported-model		
			knowledge-base		
			model-copy-job		
			model-customization-job		
			model-evaluation-job		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			model-import-job		
			model-invocation-job		
			prompt		
			prompt-router		
			prompt-version		
			provisioned-model		
			session		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para desmarcar um recurso Bedrock	Tags	agent		
			agent-alias		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			application-inference-profile		
			async-invoke		
			automated-reasoning-policy		
			automated-reasoning-policy-version		
			blueprint		
			custom-model		
			custom-model-deployment		
			data-automation-invocation-job		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			data-automation-project		
			evaluation-job		
			flow		
			flow-alias		
			guardrail		
			imported-model		
			knowledge-base		
			model-copy-job		
			model-customization-job		
			model-evaluation-job		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			model-import-job		
			model-invocation-job		
			prompt		
			prompt-router		
			prompt-version		
			provisioned-model		
			session		
				aws:TagKeys	
UpdateAgent	Concede permissão para atualizar um agente existente	Gravar	agent*		
UpdateAgentActionGroup	Concede permissão para atualizar um grupo de ação existente	Gravar	agent*		
UpdateAgentAlias	Concede permissão para atualizar uma alias existente	Gravar	agent-alias*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateAgentCollaborator	Concede permissão para atualizar um colaborador existente	Gravar	agent*		
UpdateAgentKnowledgeBase	Concede permissão para atualizar uma base de conhecimento associada a um agente	Gravar	agent*		
			knowledge-base*		
UpdateAutomatedReasoningPolicy	Concede permissão para atualizar uma política de raciocínio automatizado	Gravar	automated-reasoning-policy*		
UpdateAutomatedReasoningPolicyAnnotations	Concede permissão para atualizar as anotações de um fluxo de trabalho de criação para uma política de raciocínio automatizada	Gravar	automated-reasoning-policy*		
UpdateAutomatedReasoningPolicyTestCase	Concede permissão para atualizar um caso de teste para a política de raciocínio automatizado	Gravar	automated-reasoning-policy*		
UpdateBlueprint	Concede permissão para atualizar um plano para automação de dados	Gravar	blueprint*		
UpdateDataAutomationProject	Concede permissão para atualizar um projeto de automação de dados	Gravar	data-automation-project*		
			blueprint		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateDataSource	Concede permissão para atualizar uma fonte de dados	Gravar	knowledge-base*		
UpdateFlow	Concede permissão para atualizar um fluxo de prompts	Gravar	flow*		
UpdateFlowAlias	Concede permissão para atualizar a configuração de um alias de um fluxo de prompts	Gravar	flow-alias*		
UpdateGuardrail	Concede permissão para atualizar uma barreira de proteção	Gravar	guardrail*		
			automated-reasoning-policy		
			automated-reasoning-policy-version		
			guardrail-profile		
UpdateKnowledgeBase	Concede permissão para atualizar uma base de conhecimento	Gravar	knowledge-base*		
UpdateMarketplaceModelEndpoint	Concede permissão para atualizar um endpoint do modelo de mercado	Gravar	bedrock-marketplace-model-endpoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdatePrompt	Concede permissão para atualizar um prompt	Gravar	prompt*		
UpdateProvisionedModelThroughput	Concede permissão para atualizar uma throughput de modelo provisionado que você criou anteriormente	Gravar	custom-model*		
			foundation-model*		
			provisioned-model*		
UpdateSession	Concede permissão para atualizar uma sessão existente	Gravar	session*		
ValidateFlowDefinition	Concede permissão para validar definições de fluxo imediato	Leitura			

Tipos de recursos definidos pelo Amazon Bedrock

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}	
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}

Tipos de recursos	ARN	Chaves de condição
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}
evaluation-job	arn:${Partition}:bedrock:${Region}:${Account}:evaluation-job/${ResourceId}	aws:ResourceTag/${TagKey}
model-invocation-job	arn:${Partition}:bedrock:${Region}:${Account}:model-invocation-job/${JobIdentifier}	aws:ResourceTag/${TagKey}
guardrail	arn:${Partition}:bedrock:${Region}:${Account}:guardrail/${GuardrailId}	aws:ResourceTag/${TagKey}
guardrail-profile	arn:${Partition}:bedrock:${Region}:${Account}:guardrail-profile/${ResourceId}	
automated-reasoning-policy	arn:${Partition}:bedrock:${Region}:${Account}:automated-reasoning-policy/${AutomatedReasoningPolicyId}	aws:ResourceTag/${TagKey}
automated-reasoning-policy-version	arn:${Partition}:bedrock:${Region}:${Account}:automated-reasoning-policy/${AutomatedReasoningPolicyId}:${AutomatedReasoningPolicyVersion}	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
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/${TagKey}
prompt-version	arn:${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	

Tipos de recursos	ARN	Chaves de condição
data-automation-project	`arn:${Partition}:bedrock:${Region}:${Account}:data-automation-project/${ProjectId}`	aws:ResourceTag/${TagKey}
blueprint	`arn:${Partition}:bedrock:${Region}:${Account}:blueprint/${BlueprintId}`	aws:ResourceTag/${TagKey}
data-automation-invocation-job	`arn:${Partition}:bedrock:${Region}:${Account}:data-automation-invocation/${JobId}`	aws:ResourceTag/${TagKey}
data-automation-profile	`arn:${Partition}:bedrock:${Region}:${Account}:data-automation-profile/${ProfileId}`	
session	`arn:${Partition}:bedrock:${Region}:${Account}:session/${SessionId}`	aws:ResourceTag/${TagKey}
custom-model-deployment	`arn:${Partition}:bedrock:${Region}:${Account}:custom-model/${ResourceId}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Bedrock

O Amazon Bedrock define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso ao criar solicitações com base no conjunto de valores permitidos para cada uma das etiquetas obrigatórias	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso às ações com base no valor da etiqueta associada ao recurso	String
aws:TagKeys	Filtra o acesso ao criar solicitações com base na presença de etiquetas obrigatórias na solicitação	ArrayOfString
bedrock:GuardrailIdentifier	Filtra o acesso GuardrailIdentifier contendo o Guardrail Arn ou o GuardrailArn: NumericVersion	ARN
bedrock:InferenceProfileArn	Filtra o acesso pelo perfil de inferência especificado	ARN
bedrock:InlineAgentName	Filtra o acesso pelos nomes de agentes embutidos, isso será usado em nomes de InvokeInlineAgent API	String
bedrock:PromptRouterArn	Filtra o acesso pelo roteador de prompt especificado	ARN
bedrock:ThirdPartyKnowledgeBaseCredentialsSecretArn	Filtra o acesso pelo secretARN que contém as credencias da plataforma de terceiros	ARN

Ações, recursos e chaves de condição para o Amazon Bedrock Agentcore

O Amazon Bedrock Agentcore (prefixo do serviço:`bedrock-agentcore`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Bedrock Agentcore
- Tipos de recursos definidos pelo Amazon Bedrock Agentcore
- Chaves de condição para Amazon Bedrock Agentcore

Ações definidas pelo Amazon Bedrock Agentcore

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AllowVendedLogDeliveryForResource [somente permissão]	Concede permissão para configurar a telemetria vendida para um recurso	Gerenciamento de permissões	memory*		
ConnectBrowserAutomationStream	Concede permissão para se conectar a um fluxo de automação do navegador	Leitura			
ConnectBrowserLiveViewStream	Concede permissão para se conectar a uma transmissão ao vivo do navegador	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAgentRuntime	Concede permissão para criar um novo tempo de execução do agente	Gravar			iam:PassRole
CreateAgentRuntimeEndpoint	Concede permissão para criar um novo endpoint de tempo de execução do agente	Gravar			
CreateApiKeyCredentialProvider	Concede permissão para criar um novo provedor de credenciais de chave de API	Gravar	apikeycredentialprovider*		
			token-vault*		
CreateBrowser	Concede permissão para criar um novo navegador personalizado	Gravar			
CreateCodeInterpreter	Concede permissão para criar um novo interpretador de código personalizado	Gravar			
CreateEvent	Concede permissão para criar um evento	Gravar	memory*		
				bedrock-agentcore:sessionId bedrock-agentcore:actorId	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateGateway	Concede permissão para criar um novo gateway	Gravar			iam:PassRole
CreateGatewayTarget	Concede permissão para criar um novo alvo em um gateway existente	Gravar	gateway*		
CreateMemory	Concede permissão para criar um recurso de memória	Gravar			iam:PassRole
CreateOauth2CredentialProvider	Concede permissão para criar um novo provedor de credenciais para acessar recursos externos com protocolo OAuth2	Gravar	oauth2credentialprovider*		
			token-vault*		
CreateWorkloadIdentity	Concede permissão para criar uma nova identidade de carga de trabalho	Gravar	workload-identity*		
			workload-identity-directory*		
DeleteAgentRuntime	Concede permissão para excluir um tempo de execução do agente	Gravar	runtime*		
DeleteAgentRuntimeEndpoint	Concede permissão para excluir um endpoint de tempo de execução do agente	Gravar	runtime*		
			runtime-endpoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteApiKeyCredentialProvider	Concede permissão para excluir um provedor de credenciais de chave de API registrado	Gravar	apikeycredentialprovider*		
			token-vault*		
DeleteBrowser	Concede permissão para excluir um navegador personalizado	Gravar	browser-custom*		
DeleteCodeInterpreter	Concede permissão para excluir um interpretador de código personalizado	Gravar	code-interpreter-custom*		
DeleteEvent	Concede permissão para excluir um evento	Gravar	memory*		
				bedrock-agentcore:sessionId bedrock-agentcore:actorId	
DeleteGateway	Concede permissão para excluir um gateway existente	Gravar	gateway*		
DeleteGatewayTarget	Concede permissão para excluir um alvo de gateway existente	Gravar	gateway*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteMemory	Concede permissão para excluir um recurso de memória	Gravar	memory*		
DeleteMemoryRecord	Concede permissão para excluir um registro de memória	Gravar	memory*		
DeleteOauth2CredentialProvider	Concede permissão para excluir um provedor de OAuth2 credenciais registrado	Gravar	oauth2credentialprovider*		
			token-vault*		
DeleteWorkloadIdentity	Concede permissão para excluir uma identidade de carga de trabalho registrada	Gravar	workload-identity*		
			workload-identity-directory*		
GetAgentRuntime	Concede permissão para obter detalhes do tempo de execução de um agente	Leitura	runtime*		
GetAgentRuntimeEndpoint	Concede permissão para obter detalhes de um endpoint de tempo de execução do agente	Leitura	runtime*		
			runtime-endpoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetApiKeyCredentialProvider	Concede permissão para buscar um provedor de credenciais de chave de API registrado pelo nome	Leitura	apikeycredentialprovider*		
			token-vault*		
GetBrowser	Concede permissão para obter detalhes de um navegador	Leitura	browser-custom*		
GetBrowserSession	Concede permissão para obter detalhes de uma sessão do navegador	Leitura	browser*		
			browser-custom*		
GetCodeInterpreter	Concede permissão para obter detalhes de um interpretador de código	Leitura	code-interpreter-custom*		
GetCodeInterpreterSession	Concede permissão para obter detalhes de uma sessão de intérprete de código	Leitura	code-interpreter*		
			code-interpreter-custom*		
GetEvent	Concede permissão para buscar um evento	Leitura	memory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				bedrock-agentcore:sessionId bedrock-agentcore:actorId	
GetGateway	Concede permissão para recuperar um gateway existente	Leitura	gateway*		
GetGatewayTarget	Concede permissão para recuperar um destino de gateway existente	Leitura	gateway*		
GetMemory	Concede permissão para buscar detalhes de um recurso de memória	Leitura	memory*		
GetMemoryRecord	Concede permissão para buscar um registro de memória	Leitura	memory*		
GetOauth2CredentialProvider	Concede permissão para buscar um provedor de OAuth2 credenciais registrado pelo nome	Leitura	oauth2credentialprovider*		
			token-vault*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetResourceApiKey	Concede permissão para recuperar uma chave de API associada a um provedor de credenciais de chave de API	Leitura	apikeycredentialprovider*		
			token-vault*		
			workload-identity*		
			workload-identity-directory*		
GetResourceOauth2Token	Concede permissão para recuperar o token de acesso com fluxo OAuth2 2LO ou 3LO para acessar recursos externos	Leitura	oauth2credentialprovider*		
			token-vault*		
			workload-identity*		
			workload-identity-directory*		
GetTokenVault	Concede permissão para buscar a configuração atual do TokenVault, incluindo as configurações de criptografia	Leitura	token-vault*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetWorkloadAccessToken	Concede permissão para recuperar um token de acesso à carga de trabalho para cargas de trabalho agentes que não atuam em nome de um usuário	Gravar	workload-identity*		
			workload-identity-directory*		
GetWorkloadAccessTokenForJWT	Concede permissão para recuperar um token de acesso à carga de trabalho para cargas de trabalho agentes que atuam em nome do usuário com o token JWT	Gravar	workload-identity*		
			workload-identity-directory*		
GetWorkloadAccessTokenForUserId	Concede permissão para recuperar um token de acesso à carga de trabalho para cargas de trabalho agentes que atuam em nome do usuário com ID de usuário	Gravar	workload-identity*		
			workload-identity-directory*		
GetWorkloadIdentity	Concede permissão para buscar detalhes de uma identidade específica da carga de trabalho, incluindo seu nome e retorno permitido OAuth2 URLs	Leitura	workload-identity*		
			workload-identity-directory*		
InvokeAgentRuntime	Concede permissão para invocar um endpoint de tempo de execução do agente	Gravar	runtime*		
			runtime-endpoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
InvokeCodeInterpreter	Concede permissão para invocar uma sessão de intérprete de código	Gravar	code-interpreter*		
			code-interpreter-custom*		
ListActors	Concede permissão para listar atores	Lista	memory*		
ListAgentRuntimeEndpoints	Concede permissão para listar endpoints de tempo de execução do agente	Lista			
ListAgentRuntimeVersions	Concede permissão para listar as versões de tempo de execução do agente	Lista			
ListAgentRuntimes	Concede permissão para listar os tempos de execução do agente	Lista			
ListApiKeyCredentialProviders	Concede permissão para listar todos os provedores de credenciais de chave de API no Token Vault	Leitura	apikeycredentialprovider*		
			token-vault*		
ListBrowserSessions	Concede permissão para listar sessões do navegador	Lista			
ListBrowsers	Concede permissão para listar navegadores	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListCodeInterpreterSessions	Concede permissão para listar sessões de intérprete de código	Lista	code-interpreter*		
			code-interpreter-custom*		
ListCodeInterpreters	Concede permissão para listar intérpretes de código	Lista			
ListEvents	Concede permissão para listar eventos	Lista	memory*		
				bedrock-agentcore:sessionId bedrock-agentcore:actorId	
ListGatewayTargets	Concede permissão para listar alvos de gateway existentes	Lista	gateway*		
ListGateways	Concede permissão para listar gateways existentes	Lista			
ListMemories	Concede permissão para listar recursos de memória	Lista			
ListMemoryRecords	Concede permissão para listar registros de memória	Lista	memory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				bedrock-agentcore:namespace bedrock-agentcore:strategyId	
ListOauth2CredentialProviders	Concede permissão para listar todos os provedores de OAuth2 credenciais no Token Vault	Leitura	oauth2credentialprovider*		
			token-vault*		
ListSessions	Concede permissão para listar sessões	Lista	memory*		
				bedrock-agentcore:actorId	
ListWorkloadIdentities	Concede permissão para listar todas as identidades de carga de trabalho na do chamador Conta da AWS	Leitura	workload-identity*		
			workload-identity-directory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RetrieveMemoryRecords	Concede permissão para recuperar registros de memória por meio de consulta semática	Lista	memory*		
				bedrock-agentcore:namespace bedrock-agentcore:strategyId	
SetTokenVaultCMK	Concede permissão para associar uma Chave Gerenciada pelo Cliente (CMK) ou uma Chave Gerenciada pelo Serviço a uma Chave Gerenciada pelo Cliente a uma Chave Gerenciada pelo Cliente TokenVault	Leitura	token-vault*		
StartBrowserSession	Concede permissão para iniciar uma nova sessão do navegador	Gravar	browser*		
			browser-custom*		
StartCodeInterpreterSession	Concede permissão para iniciar uma nova sessão de intérprete de código	Gravar	code-interpreter*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			code-interpreter-custom*		
StopBrowserSession	Concede permissão para interromper uma sessão do navegador	Gravar	browser*		
			browser-custom*		
StopCodeInterpreterSession	Concede permissão para interromper uma sessão do interpretador de código	Gravar	code-interpreter*		
			code-interpreter-custom*		
SynchronizeGatewayTargets [somente permissão]	Concede permissão para habilitar a pesquisa em gateways	Gerenciamento de permissões	gateway*		
UpdateAgentRuntime	Concede permissão para atualizar o tempo de execução de um agente	Gravar	runtime*		iam:PassRole
UpdateAgentRuntimeEndpoint	Concede permissão para atualizar um endpoint de tempo de execução do agente	Gravar	runtime*		
			runtime-endpoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateApiKeyCredentialProvider	Concede permissão para atualizar um provedor de credenciais de chave de API existente	Gravar	apikeycredentialprovider*		
			token-vault*		
UpdateBrowserStream	Concede permissão para atualizar o status do fluxo da sessão do navegador	Gravar	browser*		
			browser-custom*		
UpdateGateway	Concede permissão para atualizar um gateway existente	Gravar	gateway*		iam:PassRole
UpdateGatewayTarget	Concede permissão para atualizar um destino de gateway existente	Gravar	gateway*		
UpdateMemory	Concede permissão para atualizar um recurso de memória	Gravar	memory*		iam:PassRole
UpdateOauth2CredentialProvider	Concede permissão para atualizar um provedor de OAuth2 credenciais existente	Gravar	oauth2credentialprovider*		
			token-vault*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateWorkloadIdentity	Concede permissão para atualizar os metadados de uma identidade de carga de trabalho existente	Gravar	workload-identity*		
			workload-identity-directory*		

Tipos de recursos definidos pelo Amazon Bedrock Agentcore

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
memory	`arn:${Partition}:bedrock-agentcore:${Region}:${Account}:memory/${MemoryId}`	
gateway	`arn:${Partition}:bedrock-agentcore:${Region}:${Account}:gateway/${GatewayId}`	
workload-identity	`arn:${Partition}:bedrock-agentcore:${Region}:${Account}:workload-identity-directory/${DirectoryId}/workload-identity/${WorkloadIdentityName}`	

Tipos de recursos	ARN	Chaves de condição
oauth2credentialprovider	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:token-vault/${TokenVaultId}/oauth2credentialprovider/${Name}	
apikeycredentialprovider	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:token-vault/${TokenVaultId}/apikeycredentialprovider/${Name}	
runtime	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:runtime/${RuntimeId}	
runtime-endpoint	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:runtime/${RuntimeId}/runtime-endpoint/${Name}	
code-interpreter-custom	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:code-interpreter-custom/${CodeInterpreterId}	
code-interpreter	arn:${Partition}:bedrock-agentcore:${Region}:aws:code-interpreter/${CodeInterpreterId}	
browser-custom	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:browser-custom/${BrowserId}	
browser	arn:${Partition}:bedrock-agentcore:${Region}:aws:browser/${BrowserId}	

Tipos de recursos	ARN	Chaves de condição
workload-identity-directory	`arn:${Partition}:bedrock-agentcore:${Region}:${Account}:workload-identity-directory/${DirectoryId}`	
token-vault	`arn:${Partition}:bedrock-agentcore:${Region}:${Account}:token-vault/${TokenVaultId}`	

Chaves de condição para Amazon Bedrock Agentcore

O Amazon Bedrock Agentcore define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
bedrock-agentcore:actorId	Filtra o acesso por ID de ator	String
bedrock-agentcore:namespace	Filtra o acesso por namespace	String
bedrock-agentcore:sessionId	Filtra o acesso por ID de sessão	String

Chaves de condição	Descrição	Tipo
bedrock-agentcore:strategyId	Filtra o acesso por ID de estratégia de memória	String

Ações, recursos e chaves de condição para o AWS Billing

AWS Billing (prefixo do serviço:`billing`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Billing
- Tipos de recursos definidos pelo AWS Billing
- Chaves de condição do AWS Billing

Ações definidas pelo AWS Billing

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateBillingView	Concede permissão para criar uma visualização de faturamento	Gravar	billingview*		
				aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
DeleteBillingView	Concede permissão para excluir uma visualização de faturamento	Gravar	billingview*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy [somente permissão]	Concede permissão para excluir uma política de recursos de visualização de faturamento	Gerenciamento de permissões	billingview*		
				aws:ResourceTag/${TagKey}	
GetBillingData [somente permissão]	Concede permissão para realizar consultas sobre informações de faturamento	Leitura			
GetBillingDetails [somente permissão]	Concede permissão para visualizar informações de faturamento detalhadas de um item de linha	Leitura			
GetBillingNotifications [somente permissão]	Concede permissão para visualizar notificações enviadas por AWS relacionadas às informações de faturamento da sua conta	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetBillingPreferences [somente permissão]	Concede permissão para visualizar preferências de cobrança, como instância reservada, planos de economia e compartilhamento de créditos	Leitura			
GetBillingView	Concede permissão para obter os metadados de uma visualização de faturamento específica	Leitura	billingview*		
				aws:ResourceTag/${TagKey}	
GetBillingViewData [somente permissão]	Concede permissão para obter dados de custo e uso para uma visualização de faturamento especificada	Leitura	billingview*		
GetContractInformation [somente permissão]	Concede permissão para visualizar as informações de contrato da conta, incluindo o número do contrato, nomes de organização do usuário final, números de ordem de compra e se a conta é usada para atender clientes do setor público	Leitura			
GetCredits [somente permissão]	Concede permissão para visualizar créditos que foram resgatados	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetIAMAccessPreference [somente permissão]	Concede permissão para recuperar o estado da preferência de faturamento do elemento Allow IAM Access	Leitura			
GetResourcePolicy	Concede permissão para obter a visualização de faturamento especificada pela política de recursos	Gerenciamento de permissões	billingview*		
				aws:ResourceTag/${TagKey}	
GetSellerOfRecord [somente permissão]	Concede permissão para recuperar o Vendedor de registro padrão da conta	Leitura			
ListBillingViews	Concede permissão para obter uma lista de todas as suas visualizações de faturamento disponíveis	Leitura			
ListSourceViewsForBillingView	Concede permissão para obter a lista de visualizações de origem para uma visualização de faturamento especificada	Lista	billingview*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource	Concede permissão para obter a lista de tags para uma visualização de faturamento específica	Leitura	billingview*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
PutContractInformation [somente permissão]	Concede permissão para definir os nomes de organização do usuário final e se a conta é usada para atender clientes do setor público nas informações de contrato da conta	Gravar			
PutResourcePolicy [somente permissão]	Concede permissão para colocar uma política de recursos de visualização de faturamento	Gerenciamento de permissões	billingview*		
				aws:ResourceTag/${TagKey}	
RedeemCredits [somente permissão]	Concede permissão para resgatar qualquer crédito AWS	Gravar			
TagResource	Concede permissão para adicionar tags a uma visualização de faturamento especificada	Tags	billingview*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permissão para remover uma tag de uma visualização de faturamento especificada	Tags	billingview*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateBillingPreferences [somente permissão]	Concede permissão para atualizar preferências de cobrança, como instância reservada, planos de economia e compartilhamento de créditos	Gravar			
UpdateBillingView	Concede permissão para atualizar uma visualização de faturamento	Gravar	billingview*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateIAMAccessPreference [somente permissão]	Concede permissão para atualizar a preferência de faturamento do elemento Allow IAM Access	Gravar			

Tipos de recursos definidos pelo AWS Billing

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
billingview	`arn:${Partition}:billing::${Account}:billingview/${ResourceId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Billing

AWS Billing define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para AWS Billing painéis de gerenciamento de custos

AWS Billing e os painéis de gerenciamento de custos (prefixo do serviço:`bcm-dashboards`) fornecem os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas por AWS Billing painéis de gerenciamento de custos
- Tipos de recursos definidos por AWS Billing painéis de gerenciamento de custos
- Chaves de condição AWS Billing e painéis de gerenciamento de custos

Ações definidas por AWS Billing painéis de gerenciamento de custos

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando

usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDashboard	Concede permissão para criar um painel	Gravar			
DeleteDashboard	Concede permissão para excluir um painel	Gravar			
GetDashboard	Concede permissão para obter informações do painel	Leitura			
GetResourcePolicy	Concede permissão para obter a política de recursos para um painel	Leitura			
ListDashboards	Concede permissão para listar informações sobre todos os painéis de um usuário	Leitura			
ListTagsForResource	Concede permissão para listar todas as tags de um recurso	Leitura			
TagResource	Concede permissão para criar uma tag para um recurso	Gravar			
UntagResource	Concede permissão para remover uma tag de um recurso	Gravar			
UpdateDashboard	Concede permissão para atualizar um painel existente	Gravar			

Tipos de recursos definidos por AWS Billing painéis de gerenciamento de custos

AWS Billing e os painéis de gerenciamento de custos não oferecem suporte à especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para permitir o acesso AWS Billing e os painéis de gerenciamento de custos, especifique `"Resource": "*"` em sua política.

Chaves de condição AWS Billing e painéis de gerenciamento de custos

O Billing and Cost Management Dashboards não tem chaves de contexto específicas do serviço que possam ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o AWS Billing And Cost Management Data Exports

AWS Billing E o Cost Management Data Exports (prefixo do serviço:`bcm-data-exports`) fornece os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Billing And Cost Management Data Exports
- Tipos de recurso definidos pelo AWS Billing And Cost Management Data Exports
- Chaves de condição para o AWS Billing And Cost Management Data Exports

Ações definidas pelo AWS Billing And Cost Management Data Exports

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando

usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateExport	Concede permissão para criar uma exportação	Gravar	table*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteExport	Concede permissão para excluir uma exportação	Gravar	export*		
				aws:ResourceTag/${TagKey}	
GetExecution	Concede permissão para obter a execução de uma exportação	Leitura	export*		
				aws:ResourceTag/${TagKey}	
GetExport	Concede permissão para obter uma exportação	Leitura	export*		
				aws:ResourceTag/${TagKey}	
GetTable	Concede permissão para obter os detalhes de uma tabela	Leitura	table*		
ListExecutions	Concede permissão para listar todas as execuções de uma exportação	Lista	export*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
ListExports	Concede permissão para listar todas as exportações	Lista			
ListTables	Concede permissão para listar todas as tabelas disponíveis	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	export*		
				aws:ResourceTag/${TagKey}	
TagResource	Concede permissão para marcar um recurso	Marcação	export*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permissão para desmarcar um recurso	Tags	export*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateExport	Concede permissão para atualizar uma exportação	Gravar	export*		
			table*		
				aws:ResourceTag/${TagKey}	

Tipos de recurso definidos pelo AWS Billing And Cost Management Data Exports

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
export	`arn:${Partition}:bcm-data-exports:${Region}:${Account}:export/${Identifier}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
table	`arn:${Partition}:bcm-data-exports:${Region}:${Account}:table/${Identifier}`	

Chaves de condição para o AWS Billing And Cost Management Data Exports

AWS Billing E as exportações de dados de gerenciamento de custos definem as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para AWS Billing And Cost Management Pricing Calculator

AWS Billing E a Calculadora de Preços de Gerenciamento de Custos (prefixo do serviço:`bcm-pricing-calculator`) fornece os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela And AWS Billing Cost Management Pricing Calculator
- Tipos de recursos definidos pelo And AWS Billing Cost Management Pricing Calculator
- Chaves de condição para And AWS Billing Cost Management Pricing Calculator

Ações definidas pela And AWS Billing Cost Management Pricing Calculator

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateBillEstimate	Concede permissão para criar uma nova estimativa de fatura. A cobrança é cobrada por estimativas de fatura bem-sucedidas	Gravar	bill-scenario		
CreateBillScenario	Concede permissão para criar um novo cenário de cobrança	Gravar			
CreateBillScenarioCommitmentModification	Concede permissão para criar novos compromissos ou remover compromissos existentes de um cenário de cobrança especificado	Gravar	bill-scenario*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateBillScenarioUsageModification	Concede permissão para criar uso no cenário de cobrança especificado	Gravar	bill-scenario*		
CreateWorkloadEstimate	Concede permissão para criar uma nova estimativa de carga de trabalho	Gravar			
CreateWorkloadEstimateUsage	Concede permissão para criar uso na estimativa de carga de trabalho especificada	Gravar	workload-estimate*		
DeleteBillEstimate	Concede permissão para excluir a estimativa da fatura	Gravar	bill-estimate*		
DeleteBillScenario	Concede permissão para excluir um cenário de cobrança	Gravar	bill-scenario*		
DeleteBillScenarioCommitmentModification	Concede permissão para excluir compromissos recém-adicionados do cenário de cobrança especificado	Gravar	bill-scenario*		
DeleteBillScenarioUsageModification	Concede permissão para excluir o uso recém-adicionado do cenário de cobrança especificado	Gravar	bill-scenario*		
DeleteWorkloadEstimate	Concede permissão para excluir a estimativa de carga de trabalho especificada	Gravar	workload-estimate*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteWorkloadEstimateUsage	Concede permissão para excluir o uso recém-adicionado da estimativa de carga de trabalho especificada	Gravar	workload-estimate*		
GetBillEstimate	Concede permissão para recuperar detalhes de uma estimativa de fatura, incluindo custo estimado	Leitura	bill-estimate*		
GetBillScenario	Concede permissão para recuperar informações associadas a um cenário de cobrança	Leitura	bill-scenario*		
GetPreferences	Concede permissão para recuperar as preferências de tipo de tarifa aplicáveis para a conta	Leitura			
GetWorkloadEstimate	Concede permissão para recuperar informações associadas a uma estimativa de carga de trabalho	Leitura	workload-estimate*		
ListBillEstimateCommitments	Concede permissão para listar compromissos associados à estimativa de fatura especificada	Lista	bill-estimate*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListBillEstimateInputCommitmentModifications	Concede permissão para listar compromissos adicionados ou removidos para uma estimativa de fatura especificada	Lista	bill-estimate*		
ListBillEstimateInputUsageModifications	Concede permissão para listar o uso adicionado ou modificado de uma estimativa de fatura especificada	Lista	bill-estimate*		
ListBillEstimateLineItems	Concede permissão para listar itens da linha de resultados para uma estimativa de fatura especificada	Lista	bill-estimate*		
ListBillEstimates	Concede permissão para listar estimativas de faturamento	Lista			
ListBillScenarioCommitmentModifications	Concede permissão para listar compromissos incluídos em um cenário de cobrança	Lista	bill-scenario*		
ListBillScenarioUsageModifications	Concede permissão para listar as linhas de uso de um cenário de cobrança especificado	Lista	bill-scenario*		
ListBillScenarios	Concede permissão para listar cenários de cobrança	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para retornar uma lista de etiquetas de um recurso	Tags			
ListWorkloadEstimateUsage	Concede permissão para listar as linhas de uso para a estimativa de carga de trabalho especificada	Lista	workload-estimate*		
ListWorkloadEstimates	Concede permissão para listar estimativas de carga de trabalho	Lista			
TagResource	Concede permissão para adicionar uma etiqueta a um recurso	Marcação		aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover uma etiqueta de um recurso	Tags		aws:TagKeys	
UpdateBillEstimate	Concede permissão para atualizar o nome da estimativa da fatura e a data e hora de vencimento	Gravar	bill-estimate*		
UpdateBillScenario	Concede permissão para atualizar o nome e a data e a hora de expiração do cenário de cobrança especificado	Gravar	bill-scenario*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateBillScenarioCommitmentModification	Concede permissão para atualizar o grupo de compromissos no cenário de cobrança especificado	Gravar	bill-scenario*		
UpdateBillScenarioUsageModification	Concede permissão para atualizar o valor de uso, a hora de uso e o grupo de uso no cenário de cobrança especificado	Gravar	bill-scenario*		
UpdatePreferences	Concede permissão para atualizar as preferências de tipo de tarifa da conta	Gravar			
UpdateWorkloadEstimate	Concede permissão para atualizar o nome e a data e a hora de expiração da estimativa de carga de trabalho especificada	Gravar	workload-estimate*		
UpdateWorkloadEstimateUsage	Concede permissão para atualizar a quantidade de uso e o grupo de uso na estimativa de carga de trabalho especificada com base no ID de uso	Gravar	workload-estimate*		

Tipos de recursos definidos pelo And AWS Billing Cost Management Pricing Calculator

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso

também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}`	

Chaves de condição para And AWS Billing Cost Management Pricing Calculator

AWS Billing E a Calculadora de Preços de Gerenciamento de Custos define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para AWS Billing as ações recomendadas do And Cost Management

AWS Billing E as ações recomendadas do gerenciamento de custos (prefixo do serviço:`bcm-recommended-actions`) fornecem os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas por And AWS Billing Cost Management Recommended Actions
- Tipos de recursos definidos por And AWS Billing Cost Management Recommended Actions
- Chaves de condição para ações recomendadas de gerenciamento de custos AWS Billing e gerenciamento de custos

Ações definidas por And AWS Billing Cost Management Recommended Actions

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListRecommendedActions	Concede permissão para listar todas as ações recomendadas	Lista			

Tipos de recursos definidos por And AWS Billing Cost Management Recommended Actions

AWS Billing E as ações recomendadas de gerenciamento de custos não oferecem suporte à especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para permitir o acesso às AWS Billing ações recomendadas do And Cost Management, especifique `"Resource": "*"` em sua política.

Chaves de condição para ações recomendadas de gerenciamento de custos AWS Billing e gerenciamento de custos

BillingAndCostManagementRecommendedActions não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o AWS Billing Conductor

AWS Billing Conductor (prefixo do serviço:`billingconductor`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Billing Conductor
- Tipos de recursos definidos pelo AWS Billing Conductor
- Chaves de condição do AWS Billing Conductor

Ações definidas pelo AWS Billing Conductor

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateAccounts	Concede permissão para associar de uma a 30 contas a um grupo de faturamento	Gravar	billinggroup*		
AssociatePricingRules	Concede permissão para associar regras de preço	Gravar	pricingplan*		
			pricingrule*		
BatchAssociateResourcesToCustomLineItem	Concede permissão para associar recursos em lote a uma porcentagem de item de linha personalizado	Gravar	customlineitem*		
BatchDisassociateResourcesFromCustomLineItem	Concede permissão para desvincular recursos em lote de uma porcentagem de item de linha personalizado	Gravar	customlineitem*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateBillingGroup	Concede permissão para criar um grupo de faturamento	Gravar	pricingplan*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateCustomLineItem	Concede permissão para criar um item de linha personalizado	Gravar	billinggroup*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePricingPlan	Concede permissão para criar um plano de preços	Gravar	pricingrule*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreatePricingRule	Concede permissão para criar uma regra de preços	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteBillingGroup	Concede permissão para excluir um grupo de faturamento	Gravar	billinggroup*		
DeleteCustomLineItem	Concede permissão para excluir um item de linha personalizado	Gravar	customlineitem*		
DeletePricingPlan	Concede permissão para excluir um plano de preços	Gravar	pricingplan*		
DeletePricingRule	Concede permissão para excluir uma regra de preço	Gravar	pricingrule*		
DisassociateAccounts	Concede permissão para desvincular de uma a 30 contas de um grupo de faturamento	Gravar	billinggroup*		
DisassociatePricingRules	Concede permissão para desvincular regras de preço	Gravar	pricingplan*		
			pricingrule*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetBillingGroupCostReport	Concede permissão para visualizar o relatório de custos do grupo de faturamento para o grupo de faturamento especificado	Leitura	billinggroup*		
ListAccountAssociations	Concede permissão para listar as contas vinculadas da conta pagante para o período de faturamento determinado, enquanto informa o grupo de faturamento ao qual as contas vinculadas pertencem	Lista			
ListBillingGroupCostReports	Concede permissão para visualizar o relatório de custos do grupo de faturamento	Leitura			
ListBillingGroups	Concede permissão para visualizar os detalhes de grupos de faturamento	Leitura			
ListCustomLineItemVersions	Concede permissão para exibir versões de um item de linha personalizado	Leitura	customlineitem*		
ListCustomLineItems	Concede permissão para visualizar detalhes de um item de linha personalizado	Leitura			
ListPricingPlans	Concede permissão para visualizar detalhes sobre planos de preços	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListPricingPlansAssociatedWithPricingRule	Concede permissão para listar planos de preço associados a uma regra de preços	Lista	pricingrule*		
ListPricingRules	Concede permissão para visualizar detalhes sobre regras de preços	Leitura			
ListPricingRulesAssociatedToPricingPlan	Concede permissão para listar regras de preço associadas a um plano de preços	Lista	pricingplan*		
ListResourcesAssociatedToCustomLineItem	Concede permissão para listar recursos associados a uma porcentagem de item de linha personalizado	Lista	customlineitem*		
ListTagsForResource	Concede permissão para listar etiquetas de um recurso	Leitura	billinggroup		
			customlineitem		
			pricingplan		
			pricingrule		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
TagResource	Concede permissão para marcar um recurso	Marcação	billinggroup		
			customlineitem		
			pricingplan		
			pricingrule		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para desmarcar um recurso	Tags	billinggroup		
			customlineitem		
			pricingplan		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			pricingrule		
				aws:TagKeys	
UpdateBillingGroup	Concede permissão para atualizar um grupo de faturamento	Gravar	billinggroup*		
UpdateCustomLineItem	Concede permissão para atualizar um item de linha personalizado	Gravar	customlineitem*		
UpdatePricingPlan	Concede permissão para atualizar um plano de preços	Gravar	pricingplan*		
UpdatePricingRule	Concede permissão para atualizar uma regra de preços	Gravar	pricingrule*		

Tipos de recursos definidos pelo AWS Billing Conductor

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
billinggroup	`arn:${Partition}:billingconductor::${Account}:billinggroup/${BillingGroupId}`	aws:ResourceTag/${TagKey}
pricingplan	`arn:${Partition}:billingconductor::${Account}:pricingplan/${PricingPlanId}`	aws:ResourceTag/${TagKey}
pricingrule	`arn:${Partition}:billingconductor::${Account}:pricingrule/${PricingRuleId}`	aws:ResourceTag/${TagKey}
customlineitem	`arn:${Partition}:billingconductor::${Account}:customlineitem/${CustomLineItemId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Billing Conductor

AWS Billing Conductor define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do console do AWS Billing

AWS Billing O console (prefixo do serviço:`aws-portal`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo console do AWS Billing
- Tipos de recurso definidos pelo console do AWS Billing
- Chaves de condição do console do AWS Billing

Ações definidas pelo console do AWS Billing

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetConsoleActionSetEnforced [somente permissão]	Concede permissão para visualizar se ações do IAM existentes ou refinadas estão sendo usadas para controlar a autorização para os consoles de Faturamento, Gerenciamento de Custos e Contas	Leitura			
ModifyAccount [somente permissão]	Permitir ou negar aos usuários do IAM permissão para modificar as configurações da conta	Gravar			
ModifyBilling [somente permissão]	Permitir ou negar aos usuários do IAM a permissão para modificar as configurações de faturamento	Gravar			
ModifyPaymentMethods [somente permissão]	Permitir ou negar aos usuários do IAM a permissão para modificar os métodos de pagamento	Gravar			
UpdateConsoleActionSetEnforced [somente permissão]	Concede permissão para alterar se ações do IAM existentes ou refinadas serão usadas para controlar a autorização para os consoles de Faturamento, Gerenciamento de Custos e Contas	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ViewAccount [somente permissão]	Permitir ou negar aos usuários do IAM a permissão para visualizar as configurações da conta	Leitura			
ViewBilling [somente permissão]	Permitir ou negar aos usuários do IAM a permissão para visualizar as páginas de faturamento no console	Leitura			
ViewPaymentMethods [somente permissão]	Permitir ou negar aos usuários do IAM a permissão para visualizar os métodos de pagamento	Leitura			
ViewUsage [somente permissão]	Permitir ou negar aos usuários do IAM permissão para visualizar relatórios AWS de uso	Leitura			

Tipos de recurso definidos pelo console do AWS Billing

AWS Billing O console não suporta a especificação de um ARN de recurso no elemento de uma `Resource` declaração de política do IAM. Para permitir acesso ao console do AWS Billing , especifique `"Resource": "*"` na política.

Chaves de condição do console do AWS Billing

O console de faturamento não tem chaves de contexto específicas do serviço que possam ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do Amazon Braket

O Amazon Braket (prefixo do serviço: `braket`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Braket
- Tipos de recursos definidos pelo Amazon Braket
- Chaves de condição do Amazon Braket

Ações definidas pelo Amazon Braket

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptUserAgreement [somente permissão]	Concede permissão para aceitar o contrato de usuário do Amazon Braket	Gravar			
CancelJob	Concede permissão para cancelar um trabalho	Gravar	job*		
CancelQuantumTask	Concede permissão para cancelar uma tarefa quântica	Gravar	quantum-task*		
CreateJob	Concede permissão para criar um trabalho	Gravar		aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:TagKeys	
CreateQuantumTask	Concede permissão para criar uma tarefa quântica	Gravar		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
GetDevice	Concede permissão para recuperar informações sobre os dispositivos disponíveis no Amazon Braket	Leitura			
GetJob	Concede permissão para recuperar trabalhos	Leitura	job*		
GetQuantumTask	Concede permissão para recuperar tarefas quânticas	Leitura	quantum-task*		
GetServiceLinkedRoleStatus [somente permissão]	Concede permissão para verificar se o perfil vinculado ao serviço Amazon Braket foi criado	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetUserAgreementStatus [somente permissão]	Concede permissão para verificar se a conta aceitou o contrato de usuário do Amazon Braket	Leitura			
ListTagsForResource	Concede permissão para listar as etiquetas que foram aplicadas ao recurso da tarefa quântica ou ao trabalho	Leitura	job		
			quantum-task		
SearchDevices	Concede permissão para pesquisar dispositivos disponíveis no Amazon Braket	Leitura			
SearchJobs	Concede permissão para pesquisar trabalhos	Leitura			
SearchQuantumTasks	Concede permissão para pesquisar tarefas quânticas	Leitura			
TagResource	Concede permissão para adicionar uma ou mais tags a uma tarefa quântica ou a um trabalho híbrido	Tags	job		
			quantum-task		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para remover uma ou mais etiquetas de um recurso de tarefa quântica ou de um trabalho. Uma etiqueta consiste em uma chave e um valor	Marcação	job		
			quantum-task		
				aws:TagKeys	

Tipos de recursos definidos pelo Amazon Braket

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
quantum-task	`arn:${Partition}:braket:${Region}:${Account}:quantum-task/${RandomId}`	aws:ResourceTag/${TagKey}
job	`arn:${Partition}:braket:${Region}:${Account}:job/${JobName}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Braket

O Amazon Braket define as chaves de condição a seguir, que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as

condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Budget Service

AWS O Budget Service (prefixo do serviço:`budgets`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Budget Service
- Tipos de recursos definidos pelo AWS Budget Service
- Chaves de condição do AWS Budget Service

Ações definidas pelo AWS Budget Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

> **Note**
>
> As ações nesta tabela não são APIs, mas, em vez disso, são permissões que concedem acesso aos orçamentos Gerenciamento de Faturamento e Custos da AWS APIs desse acesso.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateBudgetAction	Concede permissão para configurar uma resposta que será executada quando seu orçamento exceder um limite de orçamento específico. A criação de uma ação orçamentária com tags também requer a permissão “orçamentos:” TagResource	Gravar	budgetAction*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteBudgetAction	Concede permissão para excluir uma ação associada a um orçamento específico	Gravar	budgetAction*		
DescribeBudgetAction	Concede permissão para recuperar os detalhes das ações de orçamento específicas associadas a um orçamento	Leitura	budgetAction*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeBudgetActionHistories	Concede permissão para recuperar uma visão histórica dos status das ações de orçamento associadas a uma ação de orçamento específica. Esses status incluem “Standby” (Em espera), “Pending” (Pendente) e “Executed” (Executado)	Leitura	budgetAction*		
DescribeBudgetActionsForAccount	Concede permissão para recuperar os detalhes de todas as ações de orçamento associadas à conta	Leitura			
DescribeBudgetActionsForBudget	Concede permissão para recuperar os detalhes de todas as ações de orçamento associadas a um orçamento	Leitura	budget*		
ExecuteBudgetAction	Concede permissão para iniciar uma ação de orçamento pendente, bem como reverter uma ação de orçamento executada anteriormente	Gravar	budgetAction*		
ListTagsForResource	Concede permissão para exibir tags de recursos para um orçamento ou ação orçamentária	Leitura	budget		
			budgetAction		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ModifyBudget	Concede permissão para criar e modificar orçamentos e editar detalhes de orçamentos. Criar um orçamento com tags também requer a permissão “orçamentos:” TagResource	Gravar	budget*		iam:CreateServiceLinkedRole
TagResource	Concede permissão para aplicar tags de recursos a um orçamento ou ação orçamentária. Também é necessário para criar um orçamento ou ação orçamentária com tags	Tags	budget		
			budgetAction		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover tags de recursos de um orçamento ou ação orçamentária	Tags	budget		
			budgetAction		
				aws:TagKeys	
UpdateBudgetAction	Concede permissão para atualizar os detalhes de uma ação de orçamento específica associada a um orçamento	Gravar	budgetAction*		iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ViewBudget	Concede permissão para exibir orçamentos e detalhes de orçamento	Leitura	budget*		billing:GetBillingViewData

Tipos de recursos definidos pelo AWS Budget Service

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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

Chaves de condição do AWS Budget Service

AWS O Budget Service define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base nas etiquetas transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra as ações com base nas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra ações com base nas chaves da etiqueta transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS BugBust

AWS BugBust (prefixo do serviço:`bugbust`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS BugBust

- Tipos de recursos definidos pelo AWS BugBust
- Chaves de condição do AWS BugBust

Ações definidas pelo AWS BugBust

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateEvent [somente permissão]	Concede permissão para criar um BugBust evento	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
EvaluateProfilingGroups [somente permissão]	Concede permissão para avaliar grupos de criação de perfil com check-in	Write	Event*		
				aws:ResourceTag/${TagKey}	
GetEvent [somente permissão]	Concede permissão para visualizar detalhes do cliente sobre um evento	Read	Event*		
				aws:ResourceTag/${TagKey}	
GetJoinEventStatus [somente permissão]	Concede permissão para ver o status da tentativa de um BugBust jogador de participar de um BugBust evento	Leitura	Event*		
				aws:ResourceTag/${TagKey}	
JoinEvent [somente permissão]	Concede permissão para participar de um evento	Write	Event*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
ListBugs [somente permissão]	Concede permissão para visualizar os bugs que foram importados para um evento sobre os quais os jogadores trabalharão	Read	Event*		codeguru-reviewer: DescribeCodeReview codeguru-reviewer: ListRecommendations
				aws:ResourceTag/${TagKey}	
ListEventParticipants [somente permissão]	Concede permissão para visualizar os participantes de um evento	Read	Event*		
				aws:ResourceTag/${TagKey}	
ListEventScores [somente permissão]	Concede permissão para visualizar as pontuações dos jogadores de um evento	Read	Event*		
				aws:ResourceTag/${TagKey}	
ListEvents [somente permissão]	Concede permissão para Listar BugBust eventos	Lista		aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListProfilingGroups [somente permissão]	Concede permissão para visualizar os grupos de criação de perfil que foram importados para um evento sobre os quais os jogadores trabalharão	Read	Event*		
				aws:ResourceTag/${TagKey}	
ListPullRequests [somente permissão]	Concede permissão para visualizar as solicitações pull usadas pelos jogadores para enviar correções para os respectivos bugs reivindicados em um evento	Read	Event*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource [somente permissão]	Concede permissão para listar as etiquetas de um recurso Bugbust	Read	Event*		
				aws:ResourceTag/${TagKey}	
TagResource [somente permissão]	Concede permissão para marcar um recurso Bugbust	Marcação	Event*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource [somente permissão]	Concede permissão para desmarcar um recurso Bugbust	Marcação	Event*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateEvent [somente permissão]	Concede permissão para atualizar um BugBust evento	Gravar	Event*		codeguru-profiler: DescribeProfilingGroup codeguru-profiler: ListProfilingGroups codeguru-reviewer: DescribeCodeReview codeguru-reviewer: ListCodeReviews codeguru-reviewer: ListRecommendations codeguru-reviewer: TagResource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					codeguru-reviewer: UnTagResource
				aws:ResourceTag/${TagKey}	
UpdateWorkItem [somente permissão]	Concede permissão para atualizar um item de trabalho como reivindicado ou não reinvidicado (bug ou grupo de criação de perfil)	Write	Event*		codeguru-reviewer: ListRecommendations
				aws:ResourceTag/${TagKey}	
UpdateWorkItemAdmin [somente permissão]	Concede permissão para atualizar o item de trabalho de um evento (bug ou grupo de criação de perfil)	Gravar	Event*		codeguru-reviewer: ListRecommendations
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pelo AWS BugBust

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações

identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
Event	`arn:${Partition}:bugbust:${Region}:${Account}:events/${EventId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS BugBust

AWS BugBust define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base nas etiquetas transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra as ações com base nas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra ações com base nas chaves da etiqueta transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Certificate Manager

AWS O Certificate Manager (prefixo do serviço:`acm`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Certificate Manager
- Tipos de recursos definidos pelo AWS Certificate Manager
- Chaves de condição do AWS Certificate Manager

Ações definidas pelo AWS Certificate Manager

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddTagsToCertificate	Concede permissão para adicionar uma ou mais etiquetas a um certificado	Marcação	certificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCertificate	Concede permissão para excluir um certificado e sua chave privada associada	Write	certificate*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeCertificate	Concede permissão para recuperar um certificado e seus metadados	Leitura	certificate*		
ExportCertificate	Concede permissão para exportar um certificado exportável para uso em qualquer lugar	Leitura	certificate*		
				acm:DomainNames	
GetAccountConfiguration	Concede permissão para recuperar a configuração em nível de conta do AWS Certificate Manager	Leitura			
GetCertificate	Concede permissão para recuperar um certificado e uma cadeia de certificados para um ARN de certificado	Leitura	certificate*		
ImportCertificate	Concede permissão para importar um certificado de terceiros para o AWS Certificate Manager (ACM)	Gravar	certificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListCertificates	Concede permissão para recuperar uma lista do certificados ARNs e do nome de domínio para cada ARN	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForCertificate	Concede permissão para listar as etiquetas que foram associadas a um certificado	Leitura	certificate*		
PutAccountConfiguration	Concede permissão para atualizar a configuração do nível da conta no AWS Certificate Manager	Gravar			
RemoveTagsFromCertificate	Concede permissão para remover uma ou mais etiquetas de um certificado	Marcação	certificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RenewCertificate	Concede permissão para renovar um certificado privado elegível	Write	certificate*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RequestCertificate	Concede permissão para solicitar um certificado público ou privado	Write		aws:RequestTag/${TagKey} aws:TagKeys acm:DomainNames acm:CertificateTransparencyLoggingPreference acm:ValidationMethod acm:KeyAlgorithm acm:CertificateAuthorityArn acm:Export	
ResendValidationEmail	Concede permissão para reenviar um e-mail para solicitar validação de propriedade de domínio	Gravar	certificate*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RevokeCertificate	Concede permissão para revogar um certificado exportável	Gravar	certificate*		
				acm:DomainNames	
UpdateCertificateOptions	Concede permissão para atualizar uma configuração de certificado. Use isto para especificar se deseja optar por entrar ou não no log de transparência do certificado	Gravar	certificate*		

Tipos de recursos definidos pelo AWS Certificate Manager

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
certificate	`arn:${Partition}:acm:${Region}:${Account}:certificate/${CertificateId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Certificate Manager

AWS O Certificate Manager define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
acm:CertificateAuthority	Filtra o acesso por certificateAuthority na solicitação. Pode ser usado para restringir de quais autoridades de certificação os certificados podem ser emitidos	String
acm:CertificateTransparencyLogging	Filtra o acesso por certificateTransparencyLogging opção na solicitação. O padrão será “ENABLED” se nenhuma chave estiver presente na solicitação	String
acm:DomainNames	Filtra o acesso por domainNames na solicitação. Essa chave pode ser usada para restringir quais domínios podem fazer parte das solicitações de certificado	ArrayOfString
acm:Export	Filtra o acesso pela opção de exportação na solicitação. Pode ser usado para restringir a criação de certificados que podem ser exportados	String
acm:KeyAlgorithm	Filtra o acesso por keyAlgorithm na solicitação	String
acm:ValidationMethod	Filtra o acesso por validationMethod na solicitação. O padrão será “EMAIL” se nenhuma chave estiver presente na solicitação	String
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Chatbot

AWS O Chatbot (prefixo do serviço:`chatbot`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Chatbot
- Tipos de recursos definidos pelo AWS Chatbot
- Chaves de condição do AWS Chatbot

Ações definidas pelo AWS Chatbot

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateToConfiguration	Concede permissão para associar um recurso a uma configuração	Gravar	ChatbotConfiguration*		
			custom-action*		
				aws:ResourceTag/${TagKey}	
CreateChimeWebhookConfiguration	Concede permissão para criar uma configuração de AWS webhook do Chatbot Chime	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
CreateCustomAction	Concede permissão para criar uma ação personalizada	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
CreateMicrosoftTeamsChannelConfiguration	Concede permissão para criar um AWS Chatbot | Configuração de canal do Microsoft Teams	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSlackChannelConfiguration	Concede permissão para criar uma configuração de canal do AWS Chatbot no Slack	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteChimeWebhookConfiguration	Concede permissão para excluir uma configuração de AWS webhook do Chatbot Chime	Gravar	ChatbotConfiguration*		
				aws:ResourceTag/${TagKey}	
DeleteCustomAction	Concede permissão para excluir uma ação personalizada	Gravar	custom-action*		
				aws:ResourceTag/${TagKey}	
DeleteMicrosoftTeamsChannelConfiguration	Concede permissão para excluir uma configuração de AWS canal do Chatbot Microsoft Teams	Gravar	ChatbotConfiguration*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteMicrosoftTeamsConfiguredTeam	Concede permissão para excluir o Microsoft Teams configurado com o AWS Chatbot em um Conta da AWS	Gravar			
DeleteMicrosoftTeamsUserIdentity	Concede permissão para excluir uma identidade de AWS usuário do Chatbot Microsoft Teams	Gravar			
DeleteSlackChannelConfiguration	Concede permissão para excluir uma configuração de canal do AWS Chatbot no Slack	Gravar	ChatbotConfiguration*		
				aws:ResourceTag/${TagKey}	
DeleteSlackUserIdentity	Concede permissão para excluir uma identidade de usuário do AWS Chatbot Slack	Gravar			
DeleteSlackWorkspaceAuthorization	Concede permissão para excluir a autorização do espaço de trabalho do Slack com o Chatbot, AWS associada a um Conta da AWS	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeChimeWebhookConfigurations	Concede permissão para listar todas as configurações do AWS Chatbot Chime Webhook em uma conta AWS	Leitura			
DescribeSlackChannelConfigurations	Concede permissão para listar todas as configurações de canais do AWS Chatbot Slack em um Conta da AWS	Leitura			
DescribeSlackChannels	Concede permissão para listar todos os canais públicos do Slack no espaço de trabalho do Slack conectado à AWS Conta integrada com o serviço Chatbot AWS	Leitura			
DescribeSlackUserIdentities	Concede permissão para descrever as identidades de usuário do AWS Chatbot Slack	Leitura			
DescribeSlackWorkspaces	Concede permissão para listar todos os workspaces autorizados do Slack conectados à AWS Conta integrada com o serviço Chatbot AWS	Leitura			
DisassociateFromConfiguration	Concede permissão para desassociar um recurso de uma configuração	Gravar	ChatbotConfiguration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			custom-action*		
				aws:ResourceTag/${TagKey}	
GetAccountPreferences	Concede permissão para recuperar as preferências da conta do AWS Chatbot	Leitura			
GetCustomAction	Concede permissão para obter uma ação personalizada	Leitura	custom-action*		
				aws:ResourceTag/${TagKey}	
GetMicrosoftTeamsChannelConfiguration	Concede permissão para obter um único AWS Chatbot Microsoft Teams Channel Configurations em um Conta da AWS	Leitura		aws:ResourceTag/${TagKey}	
GetMicrosoftTeamsOauthParameters	Concede permissão para gerar OAuth parâmetros para solicitar que o OAuth código do Microsoft Teams seja usado pelo serviço AWS Chatbot	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSlackOauthParameters	Concede permissão para gerar OAuth parâmetros para solicitar que o OAuth código do Slack seja usado pelo serviço AWS Chatbot	Leitura			
ListAssociations	Concede permissão para listar recursos associados a uma configuração	Leitura	ChatbotConfiguration*		
ListCustomActions	Concede permissão para listar ações personalizadas	Lista			
ListMicrosoftTeamsChannelConfigurations	Concede permissão para listar todas as configurações de canais AWS do Chatbot Microsoft Teams em um Conta da AWS	Leitura			
ListMicrosoftTeamsConfiguredTeams	Concede permissão para listar todas as Microsoft Teams conectadas à AWS Conta integrada ao serviço Chatbot AWS	Leitura			
ListMicrosoftTeamsUserIdentities	Concede permissão para descrever as identidades de usuário AWS do Chatbot Microsoft Teams	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar todas as tags associadas à configuração do canal do AWS Chatbot	Leitura			
RedeemMicrosoftTeamsOauthCode	Concede permissão para resgatar parâmetros gerados anteriormente com a Microsoft APIs, para adquirir OAuth tokens a serem usados pelo serviço Chatbot AWS	Gravar			
RedeemSlackOauthCode	Concede permissão para resgatar parâmetros gerados anteriormente com a API do Slack, para adquirir OAuth tokens para serem usados pelo serviço Chatbot AWS	Gravar			
TagResource	Concede permissão para criar tags na configuração do canal do AWS Chatbot	Tags	ChatbotConfiguration		
			custom-action		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para remover tags na configuração do canal do AWS Chatbot	Tags	ChatbotConfiguration		
			custom-action		
				aws:TagKeys	
UpdateAccountPreferences	Concede permissão para atualizar as preferências da conta do AWS Chatbot	Gravar			
UpdateChimeWebhookConfiguration	Concede permissão para atualizar uma configuração de AWS webhook do Chatbot Chime	Gravar	ChatbotConfiguration*		
				aws:ResourceTag/${TagKey}	
UpdateCustomAction	Concede permissão para atualizar uma ação personalizada	Gravar	custom-action*		
				aws:ResourceTag/${TagKey}	
UpdateMicrosoftTeamsChannelConfiguration	Concede permissão para atualizar uma configuração de AWS canal do Chatbot Microsoft Teams	Gravar	ChatbotConfiguration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
UpdateSlackChannelConfiguration	Concede permissão para atualizar uma configuração de canal do AWS Chatbot no Slack	Gravar	ChatbotConfiguration*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pelo AWS Chatbot

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
ChatbotConfiguration	`arn:${Partition}:chatbot::${Account}:chat-configuration/${ConfigurationType}/${ChatbotConfigurationName}`	aws:ResourceTag/${TagKey}
custom-action	`arn:${Partition}:chatbot::${Account}:custom-action/${ActionName}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Chatbot

AWS O Chatbot define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Chime

O Amazon Chime (prefixo do serviço: `chime`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Chime
- Tipos de recursos definidos pelo Amazon Chime

- Chaves de condição do Amazon Chime

Ações definidas pelo Amazon Chime

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptDelegate	Concede permissão para aceitar o convite de delegado para compartilhar o gerenciamento de uma conta do Amazon Chime com outra conta AWS	Gravar			
ActivateUsers	Concede permissão para ativar os usuários em uma conta Enterprise do Amazon Chime	Write			
AddDomain	Concede permissão para adicionar um domínio à sua conta do Amazon Chime	Write			
AddOrUpdateGroups	Concede permissão para adicionar novos grupos de usuários do Active Directory ou Okta, ou atualizar os existentes, associados à sua conta Enterprise do Amazon Chime.	Gravar			
AssociateChannelFlow	Concede permissão para associar um fluxo de um canal	Gravar	app-instance-bot*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			app-instance-user*		
			channel*		
			channel-flow*		
AssociatePhoneNumberWithUser	Concede permissão para associar um número de telefone a um usuário do Amazon Chime	Write			
AssociatePhoneNumbersWithVoiceConnector	Concede permissão para associar vários números de telefone a um Amazon Chime Voice Connector	Write	voice-connector*		
AssociatePhoneNumbersWithVoiceConnectorGroup	Concede permissão para associar vários números de telefone a um grupo do Amazon Chime Voice Connector	Gravar			
AssociateSigninDelegateGroupsWithAccount	Concede permissão para associar os grupos delegados de login especificados à conta especificada do Amazon Chime	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateVoiceConnectorConnect [somente permissão]	Concede permissão para associar a instância especificada do Amazon Connect a um Amazon Chime Voice Connector	Gravar			
AuthorizeDirectory	Concede permissão para autorizar um Active Directory para sua conta Enterprise do Amazon Chime	Write			
BatchCreateAttendee	Concede permissão para criar novos participantes de uma reunião ativa do Amazon Chime SDK	Gravar	meeting*		
BatchCreateChannelMembership	Concede permissão para adicionar vários usuários e bots a um canal	Gravar	app-instance-bot*		
			app-instance-user*		
			channel*		
BatchCreateRoomMembership	Concede permissão para adição de membros da sala em lote	Write			
BatchDeletePhoneNumber	Concede permissão para mover até 50 números de telefone para a fila de exclusão	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchSuspendUser	Concede permissão para suspender até 50 usuários de uma conta LWA Team ou Enterprise do Amazon Chime	Write			
BatchUnsuspendUser	Concede permissão para remover a suspensão de até 50 usuários suspensos anteriormente para a conta LWA Enterprise especificada do Amazon Chime.	Gravar			
BatchUpdateAttendeeCapabilitiesExcept	Concede permissão para atualização AttendeeCapabilities , exceto os recursos listados em uma ExcludedAttendeeIds tabela	Gravar	meeting*		
BatchUpdatePhoneNumber	Concede permissão para atualizar os detalhes do número de telefone dentro do UpdatePhoneNumberRequestItem objeto para até 50 números de telefone	Gravar			
BatchUpdateUser	Concede permissão para atualizar os detalhes do usuário dentro do UpdateUserRequestItem objeto para até 20 usuários para a conta especificada do Amazon Chime	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ChannelFlowCallback	Concede permissão para retorno de chamada para uma mensagem em um canal	Gravar	channel*		
Connect	Concede permissão para estabelecer uma conexão de soquete da Web para o usuário da instância da aplicação ao endpoint da sessão de mensagens.	Write	app-instance-user*		
ConnectDirectory	Concede permissão para conectar um Active Directory à sua conta Enterprise do Amazon Chime.	Gravar			ds:ConnectDirectory
CreateAccount	Concede permissão para criar uma conta do Amazon Chime sob a autoridade do administrador Conta da AWS	Gravar			
CreateApiKey	Concede permissão para criar uma chave de acesso SCIM para sua conta do Amazon Chime e para a configuração do Okta	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAppInstance	Concede permissão para criar uma instância de aplicativo nos controles de acesso Conta da AWS (baseados em tags) só são compatíveis com identity-chime. <region>.amazonaws.com (endpoints)	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAppInstanceAdmin	Concede permissão para promover um usuário ou bot a AppInstanceAdmin	Gravar	app-instance* app-instance-bot* app-instance-user*		
CreateAppInstanceBot	Concede permissão para criar um bot dentro de um sistema AppInstance (os controles de acesso baseados em tags) são suportados somente no identity-chime. <region>.amazonaws.com (endpoints)	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAppInstanceUser	Concede permissão para criar um usuário dentro de um sistema AppInstance (os controles de acesso baseados em tags são suportados somente no identity-chime). <region>.amazonaws.com (endpoints)	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAttendee	Concede permissão para criar um novo participante de uma reunião ativa do Amazon Chime SDK	Write	meeting*		
CreateBot	Concede permissão para criar um bot para uma conta Enterprise do Amazon Chime	Gravar			
CreateCDRBucket	Concede permissão para criar um novo bucket do S3 de registro de detalhes da chamada	Gravar			s3:CreateBucket s3:ListAllMyBuckets
CreateChannel	Concede permissão para criar um canal para uma instância de aplicativo nos controles de acesso Conta da AWS (baseados em tags) só são compatíveis com messaging-chime. <region>.amazonaws.com (endpoints)	Gravar	app-instance-bot*		
			app-instance-user*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateChannelBan	Concede permissão para banir um usuário ou bot de um canal	Gravar	app-instance-bot*		
			app-instance-user*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			channel*		
CreateChannelFlow	Concede permissão para criar um fluxo de canal para uma instância de aplicativo nos controles de acesso Conta da AWS (baseados em tags) só são compatíveis com messaging-chime. <region>. amazonaws.com (endpoints)	Gravar	app-instance*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateChannelMembership	Concede permissão para adicionar um usuário ou bot a um canal	Gravar	app-instance-bot*		
			app-instance-user*		
			channel*		
CreateChannelModerator	Concede permissão para criar um moderador de canal	Gravar	app-instance-bot*		
			app-instance-user*		
			channel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateConnectAnalyticsConnector [somente permissão]	Concede permissão para criar um conector Amazon Connect Analytics no Amazon Connect. Os controles de acesso Conta da AWS (baseados em tags) são suportados somente em voice-chime. <region>. amazonaws.com (endpoints)	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	chime:CreateVoiceConnector
CreateConnectCallTransferConnector [somente permissão]	Concede permissão para criar um conector de transferência de chamadas do Amazon Connect no Amazon Connect. Os controles de acesso Conta da AWS (baseados em tags) são suportados somente no sinal de voz. <region>. amazonaws.com (endpoints)	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	chime:CreateVoiceConnector
CreateMediaCapturePipeline	Concede permissão para criar um pipeline de captura de mídia (os controles de acesso baseados em tags são suportados apenas no media-pipelines-chime. <region>. amazonaws.com (endpoints)	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	s3:GetBucketPolicy

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateMediaConcatenationPipeline	Concede permissão para criar um pipeline de concatenação de mídia (controles de acesso baseados em tags são suportados apenas no. media-pipelines-chime <region>. amazonaws.com (endpoints)	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	s3:GetBucketPolicy
CreateMediaInsightsPipeline	Concede permissão para criar um pipeline de insights de mídia (controles de acesso baseados em tags são suportados apenas no media-pipelines-chime. <region>. amazonaws.com (endpoints)	Gravar	media-insights-pipeline-configuration*		chime:TagResource kinesisvideo:DescribeStream
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateMediaInsightsPipelineConfiguration	Concede permissão para criar uma configuração de pipeline de insights de mídia (controles de acesso baseados em tags são suportados apenas no media-pipelines-chime.<region>.amazonaws.com (endpoints)	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	chime:TagResource iam:PassRole kinesis:DescribeStream s3:ListBucket
CreateMediaLiveConnectorPipeline	Concede permissão para criar um pipeline de conectores ao vivo de mídia (os controles de acesso baseados em tags são suportados apenas no media-pipelines-chime. <region>.amazonaws.com (endpoints)	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateMediaPipelineKinesisVideoStreamPool	Concede permissão para criar um pool de streaming de vídeo do Kinesis (os controles de acesso baseados em tags são suportados somente no. media-pipelines-chime <region>.amazonaws.com (endpoints)	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	kinesis:DescribeStream kinesisvideo:CreateStream kinesisvideo:GetDataEndpoint kinesisvideo:ListStreams
CreateMediaStreamPipeline	Concede permissão para criar um pipeline de fluxo de mídia (os controles de acesso baseados em tags são suportados apenas no media-pipelines-chime. <region>. amazonaws.com (endpoints)	Gravar	media-pipeline-kinesis-video-stream-pool*		kinesisvideo:DescribeStream kinesisvideo:GetDataEndpoint kinesisvideo:PutMedia

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateMeeting	Concede permissão para criar uma reunião na região de mídia especificada, sem participantes iniciais (controles de acesso baseados em tags são compatíveis apenas com endpoints meetings-chime.<region>.amazonaws.com)	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateMeetingDialOut	Concede permissão para ligar para um número de telefone para participar da reunião especificada do SDK do Amazon Chime	Gravar	meeting*		
CreateMeetingWithAttendees	Concede permissão para criar uma reunião na região de mídia especificada, com um conjunto de participantes (controles de acesso baseados em tags são compatíveis apenas com endpoints meetings-chime.<region>.amazonaws.com)	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreatePhoneNumberOrder	Concede permissão para criar um pedido de número de telefone com as operadoras	Write			
CreateProxySession	Concede permissão ao Amazon Chime Voice Connector especificado para criar uma sessão de proxy	Write	voice-connector*		
CreateRoom	Concede permissão para criar uma sala	Write			
CreateRoomMembership	Concede permissão para adicionar um membro da sala	Gravar			
CreateSipMediaApplication	Concede permissão para criar um aplicativo de mídia Amazon Chime SIP no Amazon Chime. Os controles de acesso Conta da AWS (baseados em tags) são suportados somente no voice-chime. <region>.amazonaws.com (endpoints)	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
CreateSipMediaApplicationCall	Concede permissão para criar uma chamada externa para o aplicativo de mídia Amazon Chime SIP sob o comando do administrador Conta da AWS	Gravar	sip-media-application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSipRule	Concede permissão para criar uma regra SIP do Amazon Chime de acordo com as regras do administrador Conta da AWS	Gravar	sip-media-application		
CreateUser	Concede permissão para criar um usuário na conta especificada do Amazon Chime	Gravar			
CreateVoiceConnector	Concede permissão para criar um conector de voz no (s) controle de acesso Conta da AWS (baseado em tag) que só é suportado no voice-chime. <region>.amazonaws.com (endpoints)	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	chime:CreateConnectAnalyticsConnector chime:CreateConnectCallTransferConnector
CreateVoiceConnectorGroup	Concede permissão para criar um grupo de conectores de voz do Amazon Chime sob o comando do administrador Conta da AWS	Gravar	voice-connector		
CreateVoiceProfile	Concede permissão para criar um perfil de voz	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateVoiceProfileDomain	Concede permissão para criar um domínio de perfil de voz (controles de acesso baseados em tags são compatíveis apenas com endpoints voice-chime.<region>.amazonaws.com)	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	chime:TagResource kms:CreateGrant kms:DescribeKey
DeleteAccount	Concede permissão para excluir a conta do Amazon Chime especificada	Gravar			
DeleteAccountOpenIdConfig	Concede permissão para excluir os OpenIdConfig atributos da sua conta do Amazon Chime	Gravar			
DeleteApiKey	Concede permissão para excluir a chave de acesso SCIM especificada associada à sua conta do Amazon Chime e à configuração do Okta	Gravar			
DeleteAppInstance	Concede permissão para excluir um AppInstance	Gravar	app-instance*		
DeleteAppInstanceAdmin	Concede permissão para rebaixar um AppInstanceAdmin para um usuário ou bot	Gravar	app-instance* app-instance-bot*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			app-instance-user*		
DeleteAppInstanceBot	Concede permissão para excluir um AppInstanceBot	Gravar	app-instance-bot*		
DeleteAppInstanceStreamingConfigurations	Concede permissão para desativar a transmissão de dados para a instância do aplicativo	Gravar	app-instance*		
DeleteAppInstanceUser	Concede permissão para excluir um AppInstanceUser	Gravar	app-instance-user*		
DeleteAttendee	Concede permissão para excluir o participante especificado de uma reunião do Amazon Chime SDK	Write	meeting*		
DeleteCDRBucket	Concede permissão para excluir um bucket do S3 de registro de detalhes da chamada da sua conta do Amazon Chime	Write			s3:DeleteBucket
DeleteChannel	Concede permissão para excluir um canal	Gravar	app-instance-bot*		
			app-instance-user*		
			channel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteChannelBan	Concede permissão para remover um usuário ou bot da lista de proibições de um canal	Gravar	app-instance-bot*		
			app-instance-user*		
			channel*		
DeleteChannelFlow	Concede permissão para excluir um fluxo de canal	Gravar	channel*		
DeleteChannelMembership	Concede permissão para remover um membro de um canal	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
DeleteChannelMessage	Concede permissão para excluir uma mensagem de canal	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
DeleteChannelModerator	Concede permissão para excluir um moderador de canal	Gravar	app-instance-bot*		
			app-instance-user*		
			channel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteDelegate	Concede permissão para excluir o Conta da AWS gerenciamento delegado da sua conta do Amazon Chime	Gravar			
DeleteDomain	Concede permissão para excluir um domínio da sua conta do Amazon Chime	Write			
DeleteEventsConfiguration	Concede permissão para excluir uma configuração de eventos para um bot receber eventos de saída	Write			
DeleteGroups	Concede permissão para excluir os grupos de usuários do Active Directory ou Okta da sua conta Enterprise do Amazon Chime	Write			
DeleteMediaCapturePipeline	Concede permissão para excluir um pipeline de captura de mídia.	Gravar	media-pipeline*		
DeleteMediaInsightsPipelineConfiguration	Concede permissão para excluir uma configuração de pipeline de insights de mídia	Gravar	media-insights-pipeline-configuration*		chime:ListVoiceConnectors
DeleteMediaPipeline	Concede permissão para excluir um pipeline de mídia	Gravar	media-pipeline*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteMediaPipelineKinesisVideoStreamPool	Concede permissão para excluir grupo de fluxo de vídeo do Kinesis	Gravar	media-pipeline-kinesis-video-stream-pool*		
DeleteMeeting	Concede permissão para excluir a reunião do Amazon Chime SDK especificada	Gravar	meeting*		
DeleteMessagingStreamingConfigurations	Concede permissão para excluir as configurações de streaming de dados de um AppInstance	Gravar	app-instance*		
DeletePhoneNumber	Concede permissão para mover um número de telefone para a fila de exclusão	Write			
DeleteProxySession	Concede permissão para excluir uma sessão de proxy ao Amazon Chime Voice Connector especificado	Write	voice-connector*		
DeleteRoom	Concede permissão para excluir uma sala	Write			
DeleteRoomMembership	Concede permissão para remover um membro da sala	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteSipMediaApplication	Concede permissão para excluir o aplicativo de mídia Amazon Chime SIP sob a autoridade do administrador Conta da AWS	Gravar	sip-media-application*		
DeleteSipRule	Concede permissão para excluir a regra SIP do Amazon Chime de acordo com as regras do administrador Conta da AWS	Gravar			
DeleteVoiceConnector	Concede permissão para excluir o Amazon Chime Voice Connector especificado	Write	voice-connector*		logs:CreateLogDelivery logs:DeleteLogDelivery logs:GetLogDelivery logs:ListLogDeliveries
DeleteVoiceConnectorEmergencyCallingConfiguration	Concede permissão para excluir a configuração de chamada de emergência ao Amazon Chime Voice Connector especificado	Gravar	voice-connector*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteVoiceConnectorExternalSystemsConfiguration	Concede permissão para excluir a configuração do sistema externo que está conectado ao Amazon Chime Voice Connector especificado	Gravar	voice-connector*		
DeleteVoiceConnectorGroup	Concede permissão para excluir o grupo do Amazon Chime Voice Connector	Write			
DeleteVoiceConnectorOrigination	Concede permissão para excluir as configurações de geração ao Amazon Chime Voice Connector especificado	Write	voice-connector*		
DeleteVoiceConnectorProxy	Concede permissão para excluir a configuração de proxy ao Amazon Chime Voice Connector especificado	Write	voice-connector*		
DeleteVoiceConnectorStreamingConfiguration	Concede permissão para excluir a configuração de streaming ao Amazon Chime Voice Connector especificado	Write	voice-connector*		
DeleteVoiceConnectorTermination	Concede permissão para excluir as configurações de encerramento ao Amazon Chime Voice Connector especificado	Write	voice-connector*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteVoiceConnectorTerminationCredentials	Concede permissão para excluir as credenciais de encerramento de SIP ao Amazon Chime Voice Connector especificado	Gravar	voice-connector*		
DeleteVoiceProfile	Concede permissão para excluir um perfil de voz	Gravar	voice-profile*		
DeleteVoiceProfileDomain	Concede permissão para excluir um domínio de perfil de voz	Gravar	voice-profile-domain*		
DeregisterAppInstanceUserEndpoint	Concede permissão para cancelar o registro de um endpoint para um usuário da instância de aplicação	Gravar	app-instance-user*		
DescribeAppInstance	Concede permissão para obter todos os detalhes de um AppInstance	Leitura	app-instance*		
DescribeAppInstanceAdmin	Concede permissão para obter todos os detalhes de um AppInstanceAdmin	Leitura	app-instance*		
			app-instance-bot*		
			app-instance-user*		
DescribeAppInstanceBot	Concede permissão para obter todos os detalhes de um AppInstanceBot	Leitura	app-instance-bot*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeAppInstanceUser	Concede permissão para obter todos os detalhes de um AppInstanceUser	Leitura	app-instance-user*		
DescribeAppInstanceUserEndpoint	Concede permissão para descrever um endpoint registrado para um usuário de instância de aplicação	Leitura	app-instance-user*		
DescribeChannel	Concede permissão para obter os detalhes completos de um canal	Read	app-instance-bot*		
			app-instance-user*		
			channel*		
DescribeChannelBan	Concede permissão para obter os detalhes completos de uma proibição de canal	Leitura	app-instance-bot*		
			app-instance-user*		
			channel*		
DescribeChannelFlow	Concede permissão para obter os detalhes completos de um fluxo de canal	Leitura	channel-flow*		
DescribeChannelMembership	Concede permissão para obter os detalhes completos de uma associação ao canal	Leitura	app-instance-bot*		
			app-instance-user*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			channel*		
DescribeChannelMembershipForAppInstanceUser	Concede permissão para obter os detalhes de um canal com base na associação do usuário ou bot especificado	Leitura	app-instance-bot*		
			app-instance-user*		
			channel*		
DescribeChannelModeratedByAppInstanceUser	Concede permissão para obter os detalhes completos de um canal moderado pelo usuário ou bot especificado	Leitura	app-instance-bot*		
			app-instance-user*		
			channel*		
DescribeChannelModerator	Concede permissão para obter os detalhes completos de um único ChannelModerator	Leitura	app-instance-bot*		
			app-instance-user*		
			channel*		
DisassociateChannelFlow	Concede permissão para desassociar um fluxo de um canal	Gravar	app-instance-bot*		
			app-instance-user*		
			channel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			channel-flow*		
DisassociatePhoneNumberFromUser	Concede permissão para desassociar o número de telefone provisionado principal do usuário especificado do Amazon Chime	Write			
DisassociatePhoneNumbersFromVoiceConnector	Concede permissão para desassociar vários números de telefone do Amazon Chime Voice Connector especificado	Write	voice-connector*		
DisassociatePhoneNumbersFromVoiceConnectorGroup	Concede permissão para desassociar vários números de telefone do grupo do Amazon Chime Voice Connector especificado	Gravar			
DisassociateSigninDelegateGroupsFromAccount	Concede permissão para desassociar os grupos delegados de login especificados da conta especificada do Amazon Chime	Gravar			
DisassociateVoiceConnectorConnect [somente permissão]	Concede permissão para desassociar a instância do Amazon Connect do Amazon Chime Voice Connector especificado	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisconnectDirectory	Concede permissão para desconectar o Active Directory da sua conta Enterprise do Amazon Chime	Write			
GetAccount	Concede permissão para obter detalhes da conta especificada do Amazon Chime	Read			
GetAccountResource	Concede permissão para obter detalhes do recurso de conta associado à sua do conta Amazon Chime	Read			
GetAccountSettings	Concede permissão para obter as configurações da conta para o ID da conta do Amazon Chime especificada	Leitura			
GetAccountWithOpenIdConfig	Concede permissão para obter os detalhes e OpenIdConfig atributos da conta da sua conta Amazon Chime	Leitura			
GetAppInstanceRetentionSettings	Concede permissão para obter configurações de retenção para uma instância de aplicativo	Read	app-instance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAppInstanceStreamingConfigurations	Concede permissão para obter as configurações de transmissão para uma instância de aplicativo	Read	app-instance*		
GetAttendee	Concede permissão para obter detalhes do participante para um ID de reunião e ID de participante especificados	Read	meeting*		
GetBot	Concede permissão para recuperar os detalhes do bot especificado	Read			
GetCDRBucket	Concede permissão para obter os detalhes de um bucket do S3 de registro de detalhes da chamada associado à sua conta do Amazon Chime	Leitura			s3:GetBucketAcl s3:GetBucketLocation s3:GetBucketLogging s3:GetBucketVersioning s3:GetBucketWebsite

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetChannelMembershipPreferences	Concede permissão para obter as preferências para uma associação ao canal	Leitura	app-instance-bot*		
			app-instance-user*		
			channel*		
GetChannelMessage	Concede permissão para obter todos os detalhes de uma mensagem de canal	Leitura	app-instance-bot*		
			app-instance-user*		
			channel*		
GetChannelMessageStatus	Concede permissão para obter o status de uma mensagem de canal	Leitura	app-instance-bot*		
			app-instance-user*		
			channel*		
GetDomain	Concede permissão para obter detalhes de um domínio associado à sua conta do Amazon Chime	Read			
GetEventsConfiguration	Concede permissão para recuperar detalhes de uma configuração de eventos para um bot receber eventos de saída	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetGlobalSettings	Concede permissão para obter configurações globais relacionadas ao Amazon Chime para o Conta da AWS	Leitura			
GetMediaCapturePipeline	Concede permissão para obter um pipeline de captura de mídia existente	Leitura	media-pipeline*		
GetMediaInsightsPipelineConfiguration	Concede permissão para obter uma configuração de pipeline de insights de mídia	Leitura	media-insights-pipeline-configuration*		
GetMediaPipeline	Concede permissão para obter um pipeline de mídia existente	Leitura	media-pipeline*		
GetMediaPipelineKinesisVideoStreamPool	Concede permissão para obter um pipeline de mídia existente	Leitura	media-pipeline-kinesis-video-stream-pool*		
GetMeeting	Concede permissão para obter o registro de reunião para um ID de reunião especificado	Read	meeting*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetMeetingDetail	Concede permissão para obter informações sobre participantes, conexão e outros detalhes de uma reunião	Read			
GetMessagingSessionEndpoint	Concede permissão para obter o endpoint para a sessão de mensagens	Leitura			
GetMessagingStreamingConfigurations	Concede permissão para obter as configurações de streaming de dados de um AppInstance	Leitura	app-instance*		
GetPhoneNumber	Concede permissão para obter detalhes do número de telefone especificado	Read			
GetPhoneNumberOrder	Concede permissão para obter detalhes do pedido de número de telefone especificado	Leitura			
GetPhoneNumberSettings	Concede permissão para obter configurações de número de telefone relacionadas ao Amazon Chime para o Conta da AWS	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetProxySession	Concede permissão para obter detalhes da sessão de proxy especificada ao Amazon Chime Voice Connector especificado	Leitura	voice-connector*		
GetRetentionSettings	Concede permissão para recuperar as configurações de retenção da conta do Amazon Chime especificada	Leitura			
GetRoom	Concede permissão para recuperar uma sala	Leitura			
GetSipMediaApplication	Concede permissão para obter detalhes do aplicativo de mídia Amazon Chime SIP sob o comando do administrador Conta da AWS	Leitura	sip-media-application*		
GetSipMediaApplicationAlexaSkillConfiguration	Concede permissão para obter as configurações do Alexa Skill para o aplicativo de mídia Amazon Chime SIP sob o comando do administrador Conta da AWS	Leitura	sip-media-application*		
GetSipMediaApplicationLoggingConfiguration	Concede permissão para obter as configurações de registro do aplicativo de mídia Amazon Chime SIP sob o comando do administrador Conta da AWS	Leitura	sip-media-application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSipRule	Concede permissão para obter detalhes da regra SIP do Amazon Chime de acordo com as regras do administrador Conta da AWS	Leitura			
GetSpeakerSearchTask	Concede permissão para obter uma tarefa de pesquisa de palestrante no recurso especificado do Amazon Chime	Leitura	media-pipeline		
			voice-connector		
GetTelephonyLimits	Concede permissão para obter limites de telefonia para o Conta da AWS	Leitura			
GetUser	Concede permissão para obter detalhes do ID de usuário especificado	Read			
GetUserActivityReportData	Concede permissão para obter um resumo das atividades do usuário na página de detalhes do usuário	Read			
GetUserByEmail	Concede permissão para obter os detalhes de um usuário do Amazon Chime com base no endereço de e-mail em uma conta Team ou Enterprise do Amazon Chime	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetUserSettings	Concede permissão para obter configurações do usuário relacionadas ao usuário do Amazon Chime especificado	Read			
GetVoiceConnector	Concede permissão ao Amazon Chime Voice Connector especificado para obter detalhes	Read	voice-connector*		
GetVoiceConnectorEmergencyCallingConfiguration	Concede permissão ao Amazon Chime Voice Connector especificado para obter detalhes da configuração de chamada de emergência	Leitura	voice-connector*		
GetVoiceConnectorExternalSystemsConfiguration	Concede permissão para obter a configuração do sistema externo que está conectado ao Amazon Chime Voice Connector especificado	Leitura	voice-connector*		
GetVoiceConnectorGroup	Concede permissão ao grupo do Amazon Chime Voice Connector especificado para obter detalhes	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetVoiceConnectorLoggingConfiguration	Concede permissão ao Amazon Chime Voice Connector especificado para obter detalhes da configuração de registro em log	Read	voice-connector*		
GetVoiceConnectorOrigination	Concede permissão ao Amazon Chime Voice Connector especificado para obter detalhes das configurações de geração	Read	voice-connector*		
GetVoiceConnectorProxy	Concede permissão ao Amazon Chime Voice Connector especificado para obter detalhes da configuração de proxy	Read	voice-connector*		
GetVoiceConnectorStreamingConfiguration	Concede permissão ao Amazon Chime Voice Connector especificado para obter detalhes da configuração de streaming	Read	voice-connector*		
GetVoiceConnectorTermination	Concede permissão ao Amazon Chime Voice Connector especificado para obter detalhes das configurações de encerramento	Read	voice-connector*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetVoiceConnectorTerminationHealth	Concede permissão ao Amazon Chime Voice Connector especificado para obter detalhes da integridade do encerramento	Leitura	voice-connector*		
GetVoiceProfile	Concede permissão para obter um perfil de voz	Leitura	voice-profile*		
GetVoiceProfileDomain	Concede permissão para obter um domínio de perfil de voz	Leitura	voice-profile-domain*		
GetVoiceToneAnalysisTask	Concede permissão para obter uma tarefa de análise de tom de voz no recurso especificado do Amazon Chime	Leitura	media-pipeline voice-connector		
InviteDelegate	Concede permissão para enviar um convite para aceitar uma solicitação de Conta da AWS delegação para uma conta do Amazon Chime	Gravar			
InviteUsers	Concede permissão para convidar até 50 usuários para a conta do Amazon Chime especificada	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
InviteUsersFromProvider	Concede permissão para convidar usuários de um provedor de terceiros para sua conta do Amazon Chime	Write			
ListAccountUsageReportData	Concede permissão para listar os dados do relatório de uso da conta do Amazon Chime	Lista			
ListAccounts	Concede permissão para listar as contas do Amazon Chime sob a autoridade do administrador Conta da AWS	Lista			
ListApiKeys	Concede permissão para listar as chaves de acesso SCIM definidas para sua conta do Amazon Chime e para a configuração do Okta	List			
ListAppInstanceAdmins	Concede permissão para listar administradores na instância do aplicativo	Lista	app-instance*		
			app-instance-bot*		
			app-instance-user*		
ListAppInstanceBots	Concede permissão para listar tudo AppInstanceBots criado em uma única instância do aplicativo	Lista	app-instance-bot*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAppInstanceUserEndpoints	Concede permissão para listar os endpoints registrados para um usuário de instância da aplicação	Lista	app-instance-user*		
ListAppInstanceUsers	Concede permissão para listar tudo AppInstanceUsers criado em uma única instância do aplicativo	Lista	app-instance-user*		
ListAppInstances	Concede permissão para listar todas as instâncias do aplicativo Amazon Chime criadas em uma única Conta da AWS	Lista	app-instance*		
ListAttendeeTags	Concede permissão para listar as etiquetas aplicadas a um recurso de participante do Amazon Chime SDK	List	meeting*		
ListAttendees	Concede permissão para listar até 100 participantes de uma reunião do Amazon Chime SDK especificada	Lista	meeting*		
ListAvailableVoiceConnectorRegions	Concede permissão para listar os disponíveis Regiões da AWS nos quais você pode criar um conector de voz do Amazon Chime SDK	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListBots	Concede permissão para listar os bots associados à conta Enterprise do Amazon Chime do administrador	List			
ListCDRBucket	Concede permissão para listar os buckets do S3 de registro de detalhes da chamada	Lista			s3:ListAllMyBuckets s3:ListBucket
ListCallingRegions	Concede permissão para listar as regiões de chamada disponíveis para o administrador Conta da AWS	Lista			
ListChannelBans	Concede permissão para listar todos os usuários e bots banidos de um canal específico	Lista	app-instance-bot*		
			app-instance-user*		
			channel*		
ListChannelFlows	Concede permissão para listar todos os fluxos de canais criados em um único Chime AppInstance	Lista	channel-flow*		
ListChannelMemberships	Concede permissão para listar todas as associações de canal em um canal	Lista	app-instance-bot*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			app-instance-user*		
			channel*		
ListChannelMembershipsForAppInstanceUser	Concede permissão para listar todos os canais dos quais um usuário ou bot específico faz parte	Lista	app-instance-bot*		
			app-instance-user*		
ListChannelMessages	Concede permissão para listar todas as mensagens em um canal	Leitura	app-instance-bot*		
			app-instance-user*		
			channel*		
ListChannelModerators	Concede permissão para listar todos os moderadores de um canal	Lista	app-instance-bot*		
			app-instance-user*		
			channel*		
ListChannels	Concede permissão para listar todos os canais criados em um único Chime AppInstance	Lista	app-instance-bot*		
			app-instance-user*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListChannelsAssociatedWithChannelFlow	Concede permissão para listar todos os canais associados a um único fluxo de canais do Chime	Lista	channel-flow*		
ListChannelsModeratedByAppInstanceUser	Concede permissão para listar todos os canais moderados por um usuário ou bot	Lista	app-instance-bot*		
			app-instance-user*		
ListDelegates	Concede permissão para listar informações do delegado da conta associada à sua conta do Amazon Chime	Lista			
ListDirectories	Concede permissão para listar Active Directories ativos hospedados no Directory Service do seu Conta da AWS	Lista			
ListDomains	Concede permissão para listar domínios associados à sua conta do Amazon Chime	List			
ListGroups	Concede permissão para listar os grupos de usuários do Active Directory ou Okta associados à sua conta Enterprise do Amazon Chime	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListMediaCapturePipelines	Concede permissão para listar pipelines de captura de mídia	Lista			
ListMediaInsightsPipelineConfigurations	Concede permissão para listar todas as configurações de pipeline de insights de mídia	Lista			
ListMediaPipelineKinesisVideoStreamPools	Concede permissão para listar pipelines de mídia	Lista			
ListMediaPipelines	Concede permissão para listar pipelines de mídia	Lista			
ListMeetingEvents	Concede permissão para listar todos os eventos que ocorreram para uma reunião especificada	Lista			
ListMeetingTags	Concede permissão para listar as etiquetas aplicadas a um recurso de reunião do SDK do Amazon Chime	Lista	meeting*		
ListMeetings	Concede permissão para listar até 100 reuniões ativas do Amazon Chime SDK	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListMeetingsReportData	Concede permissão para listar as reuniões que terminaram durante o intervalo de datas especificado	Lista			
ListPhoneNumberOrders	Concede permissão para listar os pedidos de números de telefone sob o comando do administrador Conta da AWS	Lista			
ListPhoneNumbers	Concede permissão para listar os números de telefone abaixo dos do administrador Conta da AWS	Lista			
ListProxySessions	Concede permissão para listar sessões de proxy ao Amazon Chime Voice Connector especificado	List	voice-connector*		
ListRoomMemberships	Concede permissão para listar todos os membros da sala	List			
ListRooms	Concede permissão para listar salas	Lista			
ListSipMediaApplications	Concede permissão para listar todos os aplicativos de mídia SIP do Amazon Chime sob o comando do administrador Conta da AWS	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListSipRules	Concede permissão para listar todas as regras SIP do Amazon Chime sob as regras do administrador Conta da AWS	Lista	sip-media-application		
ListSubChannels	Concede permissão para listar tudo SubChannels em um único canal	Lista	app-instance-bot*		
			app-instance-user*		
			channel*		
ListSupportedPhoneNumberCountries	Concede permissão para listar os países com números de telefone suportados pelo Conta da AWS	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas aplicadas a um recurso do Amazon Chime	Leitura	app-instance		
			app-instance-bot		
			app-instance-user		
			channel		
			channel-flow		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			media-insights-pipeline-configuration		
			media-pipeline		
			media-pipeline-kinesis-video-stream-pool		
			meeting		
			sip-media-application		
			voice-connector		
			voice-profile-domain		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListUsers	Concede permissão para listar os usuários que pertencem à conta do Amazon Chime especificada	Lista			
ListVoiceConnectorGroups	Concede permissão para listar os grupos do Amazon Chime Voice Connector sob o comando do administrador Conta da AWS	Lista			
ListVoiceConnectorTerminationCredentials	Concede permissão para listar as credenciais de encerramento de SIP ao Amazon Chime Voice Connector especificado	Lista	voice-connector*		
ListVoiceConnectors	Concede permissão para listar os conectores de voz do Amazon Chime sob a autoridade do administrador Conta da AWS	Lista			
ListVoiceProfileDomains	Concede permissão para listar os domínios de perfil de voz	Lista			
ListVoiceProfiles	Concede permissão para listar perfis de voz	Lista	voice-profile-domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
LogoutUser	Concede permissão para encerrar a sessão do usuário especificado de todos os dispositivos nos quais ele esteja conectado no momento	Write			
PutAppInstanceRetentionSettings	Concede permissão para habilitar a retenção de dados para a instância do aplicativo	Write	app-instance*		
PutAppInstanceStreamingConfigurations	Concede permissão para configurar a transmissão de dados para a instância do aplicativo	Gravar	app-instance*		
PutAppInstanceUserExpirationSettings	Concede permissão para colocar configurações de expiração para um AppInstanceUser	Gravar	app-instance-user*		
PutChannelExpirationSettings	Concede permissão para colocar as configurações de expiração de um canal	Gravar	app-instance-user*		
			channel*		
PutChannelMembershipPreferences	Concede permissão para colocar as preferências de uma associação do canal	Gravar	app-instance-bot*		
			app-instance-user*		
			channel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutEventsConfiguration	Concede permissão para atualizar os detalhes de uma configuração de eventos para um bot receber eventos de saída	Gravar			
PutMessagingStreamingConfigurations	Concede permissão para colocar as configurações de streaming de dados de um AppInstance	Gravar	app-instance*		
PutRetentionSettings	Concede permissão para criar ou atualizar as configurações de retenção da conta do Amazon Chime especificada	Gravar			
PutSipMediaApplicationAlexaSkillConfiguration	Concede permissão para atualizar as configurações do Alexa Skill para o aplicativo de mídia Amazon Chime SIP sob o comando do administrador Conta da AWS	Gravar	sip-media-application*		
PutSipMediaApplicationLoggingConfiguration	Concede permissão para atualizar as configurações de registro do aplicativo de mídia Amazon Chime SIP sob o comando do administrador Conta da AWS	Gravar	sip-media-application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutVoiceConnectorEmergencyCallingConfiguration	Concede permissão ao Amazon Chime Voice Connector especificado para adicionar a configuração de chamada de emergência	Gravar	voice-connector*		
PutVoiceConnectorExternalSystemsConfiguration	Concede permissão para atualizar a configuração do sistema externo que está conectado ao Amazon Chime Voice Connector especificado	Gravar	voice-connector*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutVoiceConnectorLoggingConfiguration	Concede permissão ao Amazon Chime Voice Connector especificado para adicionar a configuração de registro em log	Write	voice-connector*		logs:CreateLogDelivery logs:CreateLogGroup logs:DeleteLogDelivery logs:DescribeLogGroups logs:GetLogDelivery logs:ListLogDeliveries
PutVoiceConnectorOrigination	Concede permissão ao Amazon Chime Voice Connector especificado para atualizar as configurações de geração	Write	voice-connector*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutVoiceConnectorProxy	Concede permissão ao Amazon Chime Voice Connector especificado para adicionar a configuração de proxy	Write	voice-connector*		
PutVoiceConnectorStreamingConfiguration	Concede permissão ao Amazon Chime Voice Connector especificado para adicionar a configuração de streaming	Write	voice-connector*		chime:GetMediaInsightsPipelineConfiguration
			media-insights-pipeline-configuration		
PutVoiceConnectorTermination	Concede permissão ao Amazon Chime Voice Connector especificado para atualizar as configurações de encerramento	Write	voice-connector*		
PutVoiceConnectorTerminationCredentials	Concede permissão ao Amazon Chime Voice Connector especificado para adicionar credenciais de encerramento de SIP	Write	voice-connector*		
RedactChannelMessage	Concede permissão para redação do conteúdo da mensagem	Gravar	app-instance-bot*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			app-instance-user*		
			channel*		
RedactConversationMessage	Concede permissão para editar a mensagem de conversa do Chime especificada	Gravar			
RedactRoomMessage	Concede permissão para editar a mensagem da sala do Chime especificada	Gravar			
RegenerateSecurityToken	Concede permissão para gerar novamente o token de segurança do bot especificado	Gravar			
RegisterAppInstanceUserEndpoint	Concede permissão para inscrever o registro de um endpoint para um usuário de instância de aplicação	Gravar	app-instance-user*		mobiletargeting:GetApp
RenameAccount	Concede permissão para modificar o nome da conta para a conta Enterprise ou Team do Amazon Chime	Write			
RenewDelegate	Concede permissão para renovar a solicitação de delegação associada a uma conta do Amazon Chime	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ResetAccountResource	Concede permissão para redefinir o recurso de conta em sua conta do Amazon Chime	Write			
ResetPersonalPIN	Concede permissão para redefinir o PIN de reunião pessoal para o usuário especificado em uma conta do Amazon Chime	Write			
RestorePhoneNumber	Concede permissão para restaurar o número de telefone especificado da fila de exclusão de volta para o inventário de números de telefone	Write			
RetrieveDataExports	Concede permissão para fazer download do arquivo que contém links para todos os anexos do usuário retornados como parte da ação "Solicitar anexos".	Leitura			
SearchAvailablePhoneNumbers	Concede permissão para pesquisar números de telefone que podem ser solicitados pela operadora	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SearchChannels	Concede permissão para pesquisar canais aos quais um AppInstanceUser pertence, ou canais de pesquisa em todo o mundo AppInstance para um AppInstaceAdmin	Lista	app-instance-bot*		
			app-instance-user*		
SendChannelMessage	Concede permissão para enviar uma mensagem para um canal específico do qual o membro faz parte	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
StartDataExport	Concede permissão para enviar a solicitação "Solicitação anexos"	Gravar			
StartMeetingTranscription	Concede permissão para iniciar a transcrição de uma reunião	Gravar			
StartSpeakerSearchTask	Concede permissão para iniciar uma tarefa de busca de palestrante no recurso especificado do Amazon Chime	Gravar	media-pipeline		
			voice-connector		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartVoiceToneAnalysisTask	Concede permissão para iniciar uma tarefa de análise de tom de voz no recurso especificado do Amazon Chime	Gravar	media-pipeline		
			voice-connector		
StopMeetingTranscription	Concede permissão para interromper a transcrição de uma reunião	Gravar			
StopSpeakerSearchTask	Concede permissão para interromper uma tarefa de busca de palestrante no recurso especificado do Amazon Chime	Gravar	media-pipeline		
			voice-connector		
StopVoiceToneAnalysisTask	Concede permissão para interromper uma tarefa de análise de tom de voz no recurso especificado do Amazon Chime	Gravar	media-pipeline		
			voice-connector		
SubmitSupportRequest	Concede permissão para enviar uma solicitação de suporte para o serviço de atendimento ao cliente	Write			
SuspendUsers	Concede permissão para suspender os usuários de uma conta Enterprise do Amazon Chime	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagAttendee	Concede permissão para aplicar as etiquetas especificadas ao participante especificado do Amazon Chime SDK	Tags	meeting*		
TagMeeting	Concede permissão para aplicar as etiquetas especificadas à reunião especificada do SDK do Amazon Chime	Tags	meeting*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
TagResource	Concede permissão para aplicar as tags especificadas ao recurso especificado (controles de acesso baseados em tags são compatíveis apenas com endpoints *-chime.<region>.amazonaws.com)	Tags	app-instance		
			app-instance-bot		
			app-instance-user		
			channel		
			channel-flow		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			media-insights-pipeline-configuration		
			media-pipeline		
			media-pipeline-kinesis-video-stream-pool		
			meeting		
			sip-media-application		
			voice-connector		
			voice-profile-domain		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UnauthorizeDirectory	Concede permissão para desautorizar um Active Directory da sua conta Enterprise do Amazon Chime	Gravar			
UntagAttendee	Concede permissão para desmarcar as etiquetas especificadas do participante especificado do SDK do Amazon Chime	Tags	meeting*		
UntagMeeting	Concede permissão para desmarcar as etiquetas especificadas da reunião especificada do SDK do Amazon Chime	Tags	meeting*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para desmarcar as tags especificadas do recurso especificado (controles de acesso baseados em tags são compatíveis apenas com endpoints *-chime.<region>.amazonaws.com)	Tags	app-instance		
			app-instance-bot		
			app-instance-user		
			channel		
			channel-flow		
			media-insights-pipeline-configuration		
			media-pipeline		
			media-pipeline-kinesis-video-stream-pool		
			meeting		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			sip-media-application		
			voice-connector		
			voice-profile-domain		
				aws:TagKeys	
UpdateAccount	Concede permissão para atualizar os detalhes de conta para a conta do Amazon Chime especificada	Gravar			
UpdateAccountOpenIdConfig	Concede permissão para atualizar os OpenIdConfig atributos da sua conta do Amazon Chime	Gravar			
UpdateAccountResource	Concede permissão para atualizar o recurso de conta em sua conta da Amazon Chime	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateAccountSettings	Concede permissão para atualizar as configurações da conta do Amazon Chime especificada	Gravar			
UpdateAppInstance	Concede permissão para atualizar AppInstance metadados	Gravar	app-instance*		
UpdateAppInstanceBot	Concede permissão para atualizar os detalhes de um AppInstanceBot	Gravar	app-instance-bot*		
UpdateAppInstanceUser	Concede permissão para atualizar os detalhes de um AppInstanceUser	Gravar	app-instance-user*		
UpdateAppInstanceUserEndpoint	Concede permissão para atualizar um endpoint registrado para um usuário de instância de aplicação	Gravar	app-instance-user*		
UpdateAttendeeCapabilities	Concede permissão para as capacidades que você deseja atualizar	Gravar	meeting*		
UpdateBot	Concede permissão para atualizar o status do bot especificado	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateCDRSettings	Concede permissão para atualizar o bucket do S3 de registro de detalhes da chamada	Write			s3:CreateBucket s3:DeleteBucket s3:ListAllMyBuckets
UpdateChannel	Concede permissão para atualizar os atributos de um canal	Gravar	app-instance-bot*		
			app-instance-user*		
			channel*		
UpdateChannelFlow	Concede permissão para atualizar um fluxo de canal	Gravar	channel-flow*		
UpdateChannelMessage	Concede permissão para atualizar o conteúdo de uma mensagem	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
UpdateChannelReadMarker	Concede permissão para definir o carimbo de data/hora para o ponto em que um usuário leu mensagens pela última vez em um canal	Gravar	app-instance-bot*		
			app-instance-user*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			channel*		
UpdateGlobalSettings	Concede permissão para atualizar as configurações globais relacionadas ao Amazon Chime para o Conta da AWS	Gravar			
UpdateMediaInsightsPipelineConfiguration	Concede permissão para atualizar o status de uma configuração de pipeline de insights de mídia	Gravar	media-insights-pipeline-configuration*		chime:ListVoiceConnectors iam:PassRole kinesis:DescribeStream s3:ListBucket
UpdateMediaInsightsPipelineStatus	Concede permissão para atualizar o status de um pipeline de insights de mídia	Gravar	media-pipeline*		
UpdateMediaPipelineKinesisVideoStreamPool	Concede permissão para atualizar grupo de fluxo de vídeo do Kinesis	Gravar	media-pipeline-kinesis-video-stream-pool*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdatePhoneNumber	Concede permissão para atualizar os detalhes do número de telefone especificado	Gravar			
UpdatePhoneNumberSettings	Concede permissão para atualizar as configurações de número de telefone relacionadas ao Amazon Chime para o Conta da AWS	Gravar			
UpdateProxySession	Concede permissão ao Amazon Chime Voice Connector especificado para atualizar uma sessão de proxy	Write	voice-connector*		
UpdateRoom	Concede permissão para atualizar uma sala	Write			
UpdateRoomMembership	Concede permissão para atualizar a função de membro da sala	Gravar			
UpdateSipMediaApplication	Concede permissão para atualizar as propriedades do aplicativo de mídia Amazon Chime SIP sob o comando do administrador Conta da AWS	Gravar	sip-media-application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateSipMediaApplicationCall	Concede permissão para atualizar uma chamada de aplicativo de mídia SIP do Amazon Chime sob o comando do administrador Conta da AWS	Gravar	sip-media-application*		
UpdateSipRule	Concede permissão para atualizar as propriedades da regra SIP do Amazon Chime de acordo com as regras do administrador Conta da AWS	Gravar	sip-media-application		
UpdateSupportedLicenses	Concede permissão para atualizar os níveis de licença com suporte disponíveis para usuários em sua conta do Amazon Chime	Write			
UpdateUser	Concede permissão para atualizar detalhes do usuário de um ID de usuário especificado	Write			
UpdateUserLicenses	Concede permissão para atualizar as licenças de seus usuários do Amazon Chime	Write			
UpdateUserSettings	Concede permissão para atualizar as configurações do usuário relacionadas ao usuário do Amazon Chime especificado	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateVoiceConnector	Concede permissão ao Amazon Chime Voice Connector especificado para atualizar os detalhes do Amazon Chime Voice Connector	Write	voice-connector*		
UpdateVoiceConnectorGroup	Concede permissão ao grupo do Amazon Chime Voice Connector especificado para atualizar os detalhes do grupo do Amazon Chime Voice Connector	Gravar	voice-connector		
UpdateVoiceProfile	Concede permissão para atualizar um perfil de voz	Gravar	voice-profile*		
UpdateVoiceProfileDomain	Concede permissão para atualizar um domínio de perfil de voz	Gravar	voice-profile-domain*		
ValidateAccountResource	Concede permissão para validar o recurso de conta em sua conta do Amazon Chime	Leitura			
ValidateE911Address	Concede permissão para validar um endereço a ser usado para chamadas 911 feitas com Amazon Chime Voice Connectors	Leitura			

Tipos de recursos definidos pelo Amazon Chime

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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/${TagKey}
channel	`arn:${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}

Tipos de recursos	ARN	Chaves de condição
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}
sip-media-application	arn:${Partition}:chime:${Region}:${AccountId}:sma/${SipMediaApplicationId}	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Chime

O Amazon Chime define as chaves de condição a seguir que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso pela chave e valor de uma etiqueta em uma solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta em uma solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS Clean Rooms

AWS O Clean Rooms (prefixo do serviço:`cleanrooms`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Clean Rooms
- Tipos de recursos definidos pelo AWS Clean Rooms
- Chaves de condição para o AWS Clean Rooms

Ações definidas pelo AWS Clean Rooms

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchGetCollaborationAnalysisTemplate	Concede permissão para exibir detalhes de analysisTemplates associados à colaboração	Leitura	analysistemplate*		cleanrooms:GetCollaborationAnalysisTemplate
			collaboration*		
BatchGetSchema	Concede permissão para visualizar detalhes de esquemas	Leitura	collaboration*		cleanrooms:GetSchema
			configuredtableassociation		
			idmappingtable		
BatchGetSchemaAnalysisRule	Concede permissão para exibir regras de análise associadas a esquemas	Leitura	collaboration*		cleanrooms:GetSchema
			configuredtableassociation		
			idmappingtable		
CreateAnalysisTemplate	Concede permissão para criar um novo modelo de análise	Gravar	analysistemplate*	aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:TagKeys	
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateCollaboration	Concede permissão para criar uma nova colaboração, um ambiente compartilhado de colaboração de dados	Gravar	collaboration*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateConfiguredAudienceModelAssociation	Concede permissão para vincular um modelo de público configurado pelo Cleanrooms ML a uma colaboração com a criação de uma nova associação	Gravar	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	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateConfiguredTable	Concede permissão para criar uma nova tabela configurada	Gravar	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 permissão para criar uma regra de análise para uma tabela configurada	Gravar	configuredtable*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateConfiguredTableAssociation	Concede permissão para vincular uma tabela configurada a uma colaboração ao criar uma nova associação	Gravar	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	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateConfiguredTableAssociationAnalysisRule	Concede permissão para criar uma regra de análise para uma associação de tabela configurada	Gravar	configuredtableassociation*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateIdMappingTable	Concede permissão para vincular um fluxo de trabalho de mapeamento de ID a uma colaboração ao criar uma tabela de mapeamento de ID	Gravar	idmappingtable*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	entityresolution:AddPolicyStatement entityresolution:GetIdMappingWorkflow
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateIdNamespaceAssociation	Concede permissão para vincular um namespace de ID de resolução de AWS entidade a uma colaboração criando uma nova associação	Gravar	idnamespaceassociation*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	entityresolution:AddPolicyStatement entityresolution:GetIdNamespace
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateMembership	Concede permissão para participar de colaborações mediante a criação de uma associação	Gravar	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

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					logs:PutResourcePolicy logs:UpdateLogDelivery s3:GetBucketLocation
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreatePrivacyBudgetTemplate	Concede permissão para criar um novo modelo de orçamento de privacidade	Gravar	membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			privacybudgettemplate*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteAnalysisTemplate	Concede permissão para excluir um modelo de análise existente	Gravar	analysistemplate*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteCollaboration	Concede permissão para excluir uma colaboração existente	Gravar	collaboration*		cleanrooms-ml:DeleteConfiguredAudienceModelPolicy cleanrooms-ml:GetConfiguredAudienceModelPolicy cleanrooms-ml:PutConfiguredAudienceModelPolicy

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteConfiguredAudienceModelAssociation	Concede permissão para excluir uma associação de modelo de público configurada existente	Gravar	configuredaudiencemodelassociation*		cleanrooms-ml:DeleteConfiguredAudienceModelPolicy cleanrooms-ml:GetConfiguredAudienceModelPolicy cleanrooms-ml:PutConfiguredAudienceModelPolicy
DeleteConfiguredTable	Concede permissão para excluir uma tabela configurada	Gravar	configuredtable*		
DeleteConfiguredTableAnalysisRule	Concede permissão para excluir uma regra de análise existente	Gravar	configuredtable*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteConfiguredTableAssociation	Concede permissão para remover uma associação de tabela configurada de uma colaboração	Gravar	configuredtableassociation*		
DeleteConfiguredTableAssociationAnalysisRule	Concede permissão para excluir uma regra de análise de associação de tabela configurada existente	Gravar	configuredtableassociation*		
DeleteIdMappingTable	Concede permissão para remover uma tabela de mapeamento de ID de uma colaboração	Gravar	idmappingtable*		entityresolution:DeletePolicyStatement
			membership*		
DeleteIdNamespaceAssociation	Concede permissão para remover uma associação de namespace de ID de uma colaboração	Gravar	idnamespaceassociation*		entityresolution:DeletePolicyStatement
			membership*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteMember	Concede permissão para excluir membros de uma colaboração	Gravar	collaboration*		cleanrooms-ml:DeleteConfiguredAudienceModelPolicy cleanrooms-ml:GetConfiguredAudienceModelPolicy cleanrooms-ml:PutConfiguredAudienceModelPolicy
DeleteMembership	Concede permissão para sair de colaborações mediante a exclusão de uma associação	Gravar	membership*		
DeletePrivacyBudgetTemplate	Concede permissão para excluir um modelo de orçamento de privacidade existente	Gravar	privacybudgettemplate*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAnalysisTemplate	Concede permissão para exibir detalhes de um modelo de análise	Leitura	analysistemplate*		
GetCollaboration	Concede permissão para visualizar detalhes de uma colaboração	Leitura	collaboration*		
GetCollaborationAnalysisTemplate	Concede permissão para exibir detalhes de um modelo de análise em uma colaboração	Leitura	analysistemplate*		
			collaboration*		
GetCollaborationConfiguredAudienceModelAssociation	Concede permissão para visualizar detalhes para uma associação de modelo de público configurada em uma colaboração	Leitura	collaboration*		
			configuredaudiencemodelassociation*		
GetCollaborationIdNamespaceAssociation	Concede permissão para obter associação de namespace de ID em uma colaboração	Leitura	collaboration*		
			idnamespaceassociation*		
GetCollaborationPrivacyBudgetTemplate	Concede permissão para exibir detalhes de um modelo de orçamento de privacidade em uma colaboração	Leitura	collaboration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			privacybudgettemplate*		
GetConfiguredAudienceModelAssociation	Concede permissão para visualizar detalhes de uma associação de modelo de público configurada	Leitura	configuredaudiencemodelassociation*		
GetConfiguredTable	Concede permissão para visualizar detalhes para uma tabela configurada	Leitura	configuredtable*		
GetConfiguredTableAnalysisRule	Concede permissão para visualizar regras de análise para uma tabela configurada	Leitura	configuredtable*		
GetConfiguredTableAssociation	Concede permissão para visualizar detalhes para uma associação de tabela configurada	Leitura	configuredtableassociation*		
GetConfiguredTableAssociationAnalysisRule	Concede permissão para exibir regras de análise de uma associação de tabela configurada	Leitura	configuredtableassociation*		
GetIdMappingTable	Concede permissão para exibir detalhes de uma tabela de mapeamento de ID	Leitura	idmappingtable*		
			membership*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetIdNamespaceAssociation	Concede permissão para exibir detalhes de uma associação de namespace de ID	Leitura	idnamespaceassociation*		entityresolution:GetIdNamespace
			membership*		
GetMembership	Concede permissão para visualizar detalhes sobre uma associação	Leitura	membership*		
GetPrivacyBudgetTemplate	Concede permissão para exibir detalhes de um modelo de orçamento de privacidade	Leitura	privacybudgettemplate*		
GetProtectedJob	Concede permissão para visualizar uma vaga protegida	Leitura	membership*		
GetProtectedQuery	Concede permissão para visualizar uma consulta protegida	Leitura	membership*		
GetSchema	Concede permissão para visualizar detalhes de um esquema	Leitura	collaboration*		
			configuredtableassociation*		
GetSchemaAnalysisRule	Concede permissão para visualizar regras de análise associadas a um esquema	Leitura	collaboration*		cleanrooms:GetSchema

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			configuredtableassociation*		
ListAnalysisTemplates	Concede permissão para listar modelos de análise disponíveis	Lista	analysistemplate*		
			membership*		
ListCollaborationAnalysisTemplates	Concede permissão para listar modelos de análise disponíveis em uma colaboração	Lista	collaboration*		
ListCollaborationConfiguredAudienceModelAssociations	Concede permissão para listar associações de modelos de público configuradas disponíveis em uma colaboração	Lista	collaboration*		
ListCollaborationIdNamespaceAssociations	Concede permissão para listar o namespace de ID em uma colaboração	Lista	collaboration*		
ListCollaborationPrivacyBudgetTemplates	Concede permissão para listar modelos de orçamento de privacidade disponíveis em uma colaboração	Lista	collaboration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListCollaborationPrivacyBudgets	Concede permissão para listar orçamentos de privacidade em uma colaboração	Lista	collaboration*		
ListCollaborations	Concede permissão para listar colaborações disponíveis	Lista			
ListConfiguredAudienceModelAssociations	Concede permissão para listar associações de modelos de público configuradas para uma associação	Lista	configuredaudiencemodelassociation*		
			membership*		
ListConfiguredTableAssociations	Concede permissão para listar associações de tabela configuradas para uma associação	Lista	configuredtableassociation*		
			membership*		
ListConfiguredTables	Concede permissão para listar as tabelas configuradas disponíveis	Lista			
ListIdMappingTables	Concede permissão para listar as tabelas de mapeamento de ID disponíveis para uma associação	Lista	idmappingtable*		
			membership*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListIdNamespaceAssociations	Concede permissão para listar associações de dados do Entity Resolution para uma associação	Lista	idnamespaceassociation*		
			membership*		
ListMembers	Concede permissão para listar os membros de uma colaboração	Lista	collaboration*		
ListMemberships	Concede permissão para listar as associações disponíveis	Lista			
ListPrivacyBudgetTemplates	Concede permissão para listar modelos de orçamento de privacidade disponíveis	Lista	membership*		
			privacybudgettemplate*		
ListPrivacyBudgets	Concede permissão para listar orçamentos de privacidade disponíveis	Lista	membership*		
ListProtectedJobs	Concede permissão para listar trabalhos protegidos	Lista	membership*		
ListProtectedQueries	Concede permissão para visualizar consultas protegidas	Lista	membership*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListSchemas	Concede permissão para visualizar os esquemas disponíveis de uma colaboração	Lista	collaboration*		
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	List	analysistemplate		
			collaboration		
			configuredaudiencemodelassociation		
			configuredtable		
			configuredtableassociation		
			membership		
			privacybudgettemplate		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PassCollaboration [somente permissão]	Concede permissão para acessar uma colaboração no contexto dos modelos personalizados do Clean Rooms ML	Leitura	collaboration*		
PassMembership [somente permissão]	Concede permissão para acessar uma associação no contexto dos modelos personalizados do Clean Rooms ML	Leitura	membership*		
PopulateIdMappingTable	Concede permissão para iniciar um Id Mapping Job em AWS Entity Resolution para gerar resultados de mapeamento de id na colaboração em salas limpas.	Gravar	idmappingtable*		entityresolution:GetIdMappingWorkflow
			membership*		
PreviewPrivacyImpact	Concede permissão para visualizar as configurações de modelos de orçamento de privacidade	Leitura	membership*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartProtectedJob	Concede permissão para iniciar trabalhos protegidos	Gravar	membership*		cleanrooms:GetCollaborationAnalysisTemplate cleanrooms:GetSchema
			analysistemplate		
			configuredtableassociation		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartProtectedQuery	Concede permissão para iniciar consultas protegidas	Gravar	membership*		cleanrooms:GetCollaborationAnalysisTemplate cleanrooms:GetSchema s3:GetBucketLocation s3:ListBucket s3:PutObject
			analysistemplate		
			configuredtableassociation		
			idmappingtable		
TagResource	Concede permissão para marcar um recurso	Marcação	analysistemplate		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			collaboration		
			configuredaudiencemodelassociation		
			configuredtable		
			configuredtableassociation		
			idmappingtable		
			idnamespaceassociation		
			membership		
			privacybudgettemplate		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para desmarcar um recurso	Tags	analysistemplate		
			collaboration		
			configuredaudiencemodelassociation		
			configuredtable		
			configuredtableassociation		
			idmappingtable		
			idnamespaceassociation		
			membership		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			privacybudgettemplate		
				aws:TagKeys	
UpdateAnalysisTemplate	Concede permissão para atualizar detalhes do modelo de análise	Gravar	analysistemplate*		
UpdateCollaboration	Concede permissão para atualizar detalhes da colaboração	Gravar	collaboration*		
UpdateConfiguredAudienceModelAssociation	Concede permissão para atualizar uma associação de modelo de público configurada	Gravar	configuredaudiencemodelassociation*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateConfiguredTable	Concede permissão para atualizar uma tabela configurada existente	Gravar	configuredtable*		athena:GetTableMetadata cleanrooms:UpdateConfiguredTableAllowedColumns cleanrooms:UpdateConfiguredTableReference glue:BatchGetPartition glue:GetDatabase glue:GetDatabases glue:GetPartition glue:GetPartitions

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					glue:GetSchemaVersion glue:GetTable glue:GetTables
UpdateConfiguredTableAllowedColumns [somente permissão]	Concede permissão para atualizar as colunas permitidas de uma tabela configurada existente	Gravar	configuredtable*		
UpdateConfiguredTableAnalysisRule	Concede permissão para atualizar regras de análise para uma tabela configurada	Gravar	configuredtable*		
UpdateConfiguredTableAssociation	Concede permissão para atualizar uma associação de tabela configurada	Gravar	configuredtableassociation*		iam:PassRole
UpdateConfiguredTableAssociationAnalysisRule	Concede permissão para atualizar regras de análise de uma associação de tabela configurada	Gravar	configuredtableassociation*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateConfiguredTableReference [somente permissão]	Concede permissão para atualizar a referência de tabela de uma tabela configurada existente	Gravar	configuredtable*		
UpdateIdMappingTable	Concede permissão para atualizar uma tabela de mapeamento de ID	Gravar	idmappingtable*		
			membership*		
UpdateIdNamespaceAssociation	Concede permissão para atualizar uma associação de entrada do Entity Resolution	Gravar	idnamespaceassociation*		entityresolution:GetIdNamespace
			membership*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateMembership	Concede permissão para atualizar detalhes de uma associação	Gravar	membership*		iam:PassRole logs:CreateLogDelivery logs:CreateLogGroup logs:DeleteLogDelivery logs:DescribeLogGroups logs:DescribeResourcePolicies logs:GetLogDelivery logs:ListLogDeliveries

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					logs:PutResourcePolicy logs:UpdateLogDelivery s3:GetBucketLocation
UpdatePrivacyBudgetTemplate	Concede permissão para atualizar detalhes do modelo de orçamento de privacidade	Gravar	privacybudgettemplate*		
UpdateProtectedJob	Concede permissão para atualizar trabalhos protegidos	Gravar	membership*		
UpdateProtectedQuery	Concede permissão para atualizar consultas protegidas	Gravar	membership*		

Tipos de recursos definidos pelo AWS Clean Rooms

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
membership	`arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}`	aws:ResourceTag/${TagKey}
privacybudgettemplate	`arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/privacybudgettemplate/${PrivacyBudgetTemplateId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o AWS Clean Rooms

AWS O Clean Rooms define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS Clean Rooms ML

AWS O Clean Rooms ML (prefixo do serviço:`cleanrooms-ml`) fornece os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Clean Rooms ML
- Tipos de recursos definidos pelo AWS Clean Rooms ML
- Chaves de condição para o AWS Clean Rooms ML

Ações definidas pelo AWS Clean Rooms ML

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar

a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelTrainedModel	Concede permissão para cancelar um modelo treinado	Gravar	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelTrainedModelInferenceJob	Concede permissão para cancelar um trabalho treinado de inferência de modelos	Gravar	TrainedModelInferenceJob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAudienceModel	Concede permissão para criar um modelo de público	Gravar	trainingdataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfiguredAudienceModel	Concede permissão para criar um modelo de público configurado	Gravar	audiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateConfiguredModelAlgorithm	Concede permissão para criar um algoritmo de modelo configurado	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfiguredModelAlgorithmAssociation	Concede permissão para criar uma associação de algoritmo de modelo configurado	Gravar	ConfiguredModelAlgorithm*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMLInputChannel	Concede permissão para criar um canal de entrada de ML	Gravar	ConfiguredModelAlgorithmAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTrainedModel	Concede permissão para criar um modelo treinado	Gravar	ConfiguredModelAlgorithmAssociation*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTrainingDataset	Concede permissão para criar um conjunto de dados de treinamento ou um público de treinamento. No Clean Rooms ML, TrainingDataset são metadados que apontam para uma tabela Glue, que é lida somente durante a criação AudienceModel	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAudienceGenerationJob	Concede permissão para excluir o trabalho de geração de público especificado e remove todos os dados associados ao trabalho	Gravar	audiencegenerationjob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAudienceModel	Concede permissão para excluir o trabalho de geração de público especificado e remove todos os dados associados ao trabalho	Gravar	audiencemodel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfiguredAudienceModel	Concede permissão para excluir o modelo de público configurado especificado	Gravar	configuredaudiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfiguredAudienceModelPolicy	Concede permissão para excluir a política de modelo de público configurado especificada	Gravar	configuredaudiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfiguredModelAlgorithm	Concede permissão para excluir um algoritmo de modelo configurado	Gravar	ConfiguredModelAlgorithm*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfiguredModelAlgorithmAssociation	Concede permissão para excluir uma associação de algoritmo de modelo configurado	Gravar	ConfiguredModelAlgorithmAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteMLConfiguration	Concede permissão para excluir uma configuração de ML	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteMLInputChannelData	Concede permissão para excluir todos os dados associados ao canal de entrada de ML	Gravar	MLInputChannel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteTrainedModelOutput	Concede permissão para excluir todas as saídas associadas ao modelo treinado	Gravar	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteTrainingDataset	Concede permissão para excluir um conjunto de dados de treinamento	Gravar	trainingdataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetAudienceGenerationJob	Concede permissão para retornar informações sobre um trabalho de geração de público	Leitura	audiencegenerationjob*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
GetAudienceModel	Concede permissão para retornar informações sobre um modelo de público	Leitura	audiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetCollaborationConfiguredModelAlgorithmAssociation	Concede permissão para retornar informações sobre uma associação de algoritmo de modelo configurado criada por qualquer membro da colaboração	Leitura	ConfiguredModelAlgorithmAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetCollaborationMLInputChannel	Concede permissão para retornar informações sobre um canal de entrada de ML criado por qualquer membro da colaboração	Leitura	MLInputChannel*		
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
GetCollaborationTrainedModel	Concede permissão para retornar informações sobre um modelo treinado criado por qualquer membro da colaboração	Leitura	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
GetConfiguredAudienceModel	Concede permissão para retornar informações sobre um modelo de público configurado	Leitura	configuredaudiencemodel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
GetConfiguredAudienceModelPolicy	Concede permissão para retornar informações sobre uma política modelo de público configurada	Leitura	configuredaudiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetConfiguredModelAlgorithm	Concede permissão para retornar informações sobre um algoritmo de modelo configurado	Leitura	ConfiguredModelAlgorithm*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetConfiguredModelAlgorithmAssociation	Concede permissão para retornar informações sobre uma associação de algoritmo de modelo configurado	Leitura	ConfiguredModelAlgorithmAssociation*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
GetMLConfiguration	Concede permissão para retornar informações sobre uma configuração de ML	Leitura		aws:RequestTag/${TagKey} aws:TagKeys	
GetMLInputChannel	Concede permissão para retornar informações sobre um canal de entrada de ML	Leitura	MLInputChannel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetTrainedModel	Concede permissão para retornar informações sobre um modelo treinado	Leitura	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetTrainedModelInferenceJob	Concede permissão para retornar informações sobre um trabalho treinado de inferência de modelos	Leitura	TrainedModelInferenceJob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetTrainingDataset	Concede permissão para retornar informações sobre um conjunto de dados de treinamento	Leitura	trainingdataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListAudienceExportJobs	Concede permissão para retornar uma lista dos trabalhos de exportação de público	Lista	audiencegenerationjob		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAudienceGenerationJobs	Concede permissão para retornar uma lista dos trabalhos de geração de público	Lista	configuredaudiencemodel		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListAudienceModels	Concede permissão para retornar uma lista dos modelos de público	Lista			
ListCollaborationConfiguredModelAlgorithmAssociations	Concede permissão para retornar uma lista de algoritmos de modelo configurados criados por qualquer membro da colaboração	Lista		aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListCollaborationMLInputChannels	Concede permissão para retornar uma lista de canais de entrada de ML criados por qualquer membro da colaboração	Lista		aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
ListCollaborationTrainedModelExportJobs	Concede permissão para retornar uma lista de trabalhos treinados de exportação de modelos iniciados por qualquer membro da colaboração	Lista	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListCollaborationTrainedModelInferenceJobs	Concede permissão para retornar uma lista de trabalhos treinados de inferência de modelos iniciados por qualquer membro da colaboração	Lista		aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
ListCollaborationTrainedModels	Concede permissão para retornar uma lista de modelos treinados criados por qualquer membro da colaboração	Lista		aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
ListConfiguredAudienceModels	Concede permissão para retornar uma lista de modelos de público configurados	Lista			
ListConfiguredModelAlgorithmAssociations	Concede permissão para retornar uma lista de associações de algoritmos de modelos configurados	Lista		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListConfiguredModelAlgorithms	Concede permissão para retornar uma lista de algoritmos de modelo configurados	Lista		aws:RequestTag/${TagKey} aws:TagKeys	
ListMLInputChannels	Concede permissão para retornar uma lista de canais de entrada de ML	Lista		aws:RequestTag/${TagKey} aws:TagKeys	
ListTagsForResource	Concede permissão para retornar uma lista de tags de um recurso fornecido	Lista	audiencegenerationjob		
			audiencemodel		
			configuredaudiencemodel		
			trainingdataset		
				aws:TagKeys aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTrainedModelInferenceJobs	Concede permissão para retornar uma lista de trabalhos treinados de inferência de modelos	Lista		aws:RequestTag/${TagKey} aws:TagKeys	
ListTrainedModelVersions	Concede permissão para retornar uma lista de versões treinadas do modelo	Lista		aws:RequestTag/${TagKey} aws:TagKeys	
ListTrainedModels	Concede permissão para devolver uma lista de modelos treinados	Lista		aws:RequestTag/${TagKey} aws:TagKeys	
ListTrainingDatasets	Concede permissão para retornar uma lista de conjuntos de dados de treinamento	Lista			
PutConfiguredAudienceModelPolicy	Concede permissão para criar ou atualizar a política de recurso de um modelo de público configurado	Gerenciamento de permissões	configuredaudiencemodel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutMLConfiguration	Concede permissão para colocar uma configuração de ML	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
StartAudienceExportJob	Concede permissão para exportar um público de um tamanho especificado depois de gerar um público	Gravar	audiencegenerationjob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartAudienceGenerationJob	Concede permissão para iniciar o trabalho de geração de público	Gravar	configuredaudiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartTrainedModelExportJob	Concede permissão para iniciar um trabalho de exportação de modelo treinado	Gravar	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartTrainedModelInferenceJob	Concede permissão para iniciar um trabalho treinado de inferência de modelos	Gravar	ConfiguredModelAlgorithmAssociation*		
			MLInputChannel*		
			TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Concede permissão para atribuir uma tag a um recurso específico	Tags	ConfiguredModelAlgorithm		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			ConfiguredModelAlgorithmAssociation		
			MLInputChannel		
			TrainedModel		
			TrainedModelInferenceJob		
			audiencegenerationjob		
			audiencemodel		
			configuredaudiencemodel		
			trainingdataset		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UnTagResource	Concede permissão para remover uma tag de um recurso específico	Tags	ConfiguredModelAlgorithm		
			ConfiguredModelAlgorithmAssociation		
			MLInputChannel		
			TrainedModel		
			TrainedModelInferenceJob		
			audiencegenerationjob		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			audiencemodel		
			configuredaudiencemodel		
			trainingdataset		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateConfiguredAudienceModel	Concede permissão para atualizar um modelo de público configurado	Gravar	configuredaudiencemodel*		
			audiencemodel		
				aws:RequestTag/${TagKey} aws:TagKeys	

Tipos de recursos definidos pelo AWS Clean Rooms ML

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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/${Members`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
	`hipId}/ml-input-channel/${ResourceId}`	
TrainedModel	`arn:${Partition}:cleanrooms-ml:${Region}:${Account}:membership/${MembershipId}/trained-model/${ResourceId}`	aws:ResourceTag/${TagKey}
TrainedModelInferenceJob	`arn:${Partition}:cleanrooms-ml:${Region}:${Account}:membership/${MembershipId}/trained-model-inference-job/${ResourceId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o AWS Clean Rooms ML

AWS O Clean Rooms ML define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Chaves de condição	Descrição	Tipo
cleanrooms-ml:CollaborationId	Filtra o acesso por ID de colaboração de salas limpas	String

Ações, recursos e chaves de condição para a API do Nuvem AWS Control

Nuvem AWS A API de controle (prefixo do serviço:`cloudformation`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Nuvem AWS Control API
- Tipos de recurso definidos pela Nuvem AWS Control API
- Chaves de condição para a Nuvem AWS Control API

Ações definidas pela Nuvem AWS Control API

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o

nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelResourceRequest	Concede permissão para cancelar solicitações de recurso em sua conta	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateResource	Concede permissão para criar recursos em sua conta	Gravar			
DeleteResource	Concede permissão para excluir recursos em sua conta	Gravar			
GetResource	Concede permissão para obter recursos em sua conta	Leitura			
GetResourceRequestStatus	Concede permissão para obter solicitações de recursos em sua conta	Leitura			
ListResourceRequests	Concede permissão para listar solicitações de recursos em sua conta	Leitura			
ListResources	Concede permissão para listar recursos em sua conta	Leitura			
UpdateResource	Concede permissão para atualizar recursos em sua conta	Gravar			

Tipos de recurso definidos pela Nuvem AWS Control API

Nuvem AWS A API de controle não é compatível com a especificação de um ARN de recurso `Resource` no elemento de uma declaração de política do IAM. Para permitir acesso à Nuvem AWS Control API, especifique `"Resource": "*"` na política.

Chaves de condição para a Nuvem AWS Control API

A Cloud Control API não tem chaves de contexto específicas do serviço que possam ser usadas no elemento `Condition` das instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do Amazon Cloud Directory

O Amazon Cloud Directory (prefixo do serviço: `clouddirectory`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Cloud Directory
- Tipos de recursos definidos pelo Amazon Cloud Directory
- Chaves de condição do Amazon Cloud Directory

Ações definidas pelo Amazon Cloud Directory

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddFacetToObject	Concede permissão para adicionar uma nova Faceta a um objeto	Gravar	directory*		
ApplySchema	Concede permissão para copiar o esquema de entrada	Gravar	directory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	publicado no Diretório com o mesmo nome e versão do esquema publicado		publishedSchema*		
AttachObject	Concede permissão para anexar um objeto existente a outro objeto existente	Gravar	directory*		
AttachPolicy	Concede permissão para anexar um objeto de política a qualquer outro objeto	Gravar	directory*		
AttachToIndex	Concede permissão para anexar o objeto especificado ao índice especificado	Gravar	directory*		
AttachTypedLink	Concede permissão para anexar um link digitado a b/w uma referência de objeto de origem e destino	Gravar	directory*		
BatchRead	Concede permissão para realizar todas as operações de leitura em um lote. Cada operação interna individual BatchRead precisa receber permissões explícitas	Leitura	directory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchWrite	Concede permissão para realizar todas as operações de gravação em um lote. Cada operação interna individual BatchWrite precisa receber permissões explícitas	Gravar	directory*		
CreateDirectory	Concede permissão para criar um Diretório copiando o esquema publicado no diretório	Gravar	publishedSchema*		
CreateFacet	Concede permissão para criar uma nova Faceta em um esquema	Gravar	appliedSchema*		
			developmentSchema*		
CreateIndex	Concede permissão para criar um objeto de índice	Gravar	directory*		
CreateObject	Concede permissão para criar um objeto em um Diretório	Gravar	directory*		
CreateSchema	Concede permissão para criar um novo esquema em estado de desenvolvimento	Gravar			
CreateTypedLinkFacet	Concede permissão para criar uma nova faceta de Link com tipo em um esquema	Gravar	appliedSchema*		
			developmentSchema*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteDirectory	Concede permissão para excluir um diretório. Apenas diretórios desabilitados podem ser excluídos	Gravar	directory*		
DeleteFacet	Concede permissão para excluir uma Faceta especificada. Todos os atributos e regras associados à faceta serão excluídos	Gravar	developmentSchema*		
DeleteObject	Concede permissão para excluir um objeto e seus atributos associados	Gravar	directory*		
DeleteSchema	Concede permissão para excluir um esquema especificado	Gravar	developmentSchema*		
			publishedSchema*		
DeleteTypedLinkFacet	Concede permissão para excluir uma determinada TypedLink Faceta. Todos os atributos e regras associados à faceta serão excluídos	Gravar	developmentSchema*		
DetachFromIndex	Concede permissão para desvincular o objeto especificado do índice especificado	Gravar	directory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DetachObject	Concede permissão para desvincular um determinado objeto do objeto pai	Gravar	directory*		
DetachPolicy	Concede permissão para desvincular uma política de um objeto	Gravar	directory*		
DetachTypedLink	Concede permissão para separar um determinado link b/w digitado, dada a referência do objeto de origem e destino	Gravar	directory*		
DisableDirectory	Concede permissão para desabilitar o diretório especificado	Gravar	directory*		
EnableDirectory	Concede permissão para habilitar o diretório especificado	Gravar	directory*		
GetAppliedSchemaVersion	Concede permissão para retornar o ARN da versão de esquema aplicado atual, incluindo a versão secundária em uso	Leitura	appliedSchema*		
GetDirectory	Concede permissão para recuperar metadados sobre um diretório	Leitura	directory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetFacet	Concede permissão para obter detalhes da faceta, como nome da faceta, atributos, regras ou ObjectType	Leitura	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
GetLinkAttributes	Concede permissão para recuperar atributos que estão associados a um link com tipo	Leitura	directory*		
GetObjectAttributes	Concede permissão para recuperar atributos em uma faceta que estão associados a um objeto	Leitura	directory*		
GetObjectInformation	Concede permissão para recuperar metadados sobre um objeto	Leitura	directory*		
GetSchemaAsJson	Concede permissão para recuperar uma representação JOSN do esquema	Leitura	appliedSchema*		
			developmentSchema*		
			publishedSchema*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetTypedLinkFacetInformation	Concede permissão para retornar informações sobre a ordem dos atributos de identidade associados a uma determinada faceta de link com tipo	Leitura	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
ListAppliedSchemaArns	Concede permissão para listar todos os esquemas aplicados a um diretório	Lista	directory*		
ListAttachedIndices	Concede permissão para listar índices anexados a um objeto	Leitura	directory*		
ListDevelopmentSchemaArns	Concede permissão para recuperar os esquemas no estado ARNs de desenvolvimento	Lista			
ListDirectories	Concede permissão para listar diretórios criados em uma conta	Lista			
ListFacetAttributes	Concede permissão para recuperar atributos anexados à faceta	Leitura	appliedSchema*		
			developmentSchema*		
			publishedSchema*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListFacetNames	Concede permissão para recuperar os nomes das facetas existentes em um esquema	Leitura	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
ListIncomingTypedLinks	Concede permissão para retornar uma lista paginada de todas as entradas de um determinado TypedLinks objeto	Leitura	directory*		
ListIndex	Concede permissão para listar objetos anexados ao índice especificado	Leitura	directory*		
ListManagedSchemaArns	Concede permissão para listar as famílias de versões principais de cada esquema gerenciado. Se o ARN de uma versão principal for fornecido como SchemaArn, as revisões de versão secundária dessa família serão listadas em vez disso	Lista			
ListObjectAttributes	Concede permissão para listar todos os atributos associados a um objeto	Leitura	directory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListObjectChildren	Concede permissão para retornar uma lista paginada de objetos filho associados a um determinado objeto	Leitura	directory*		
ListObjectParentPaths	Concede permissão para recuperar todos os caminhos pai disponíveis de qualquer tipo de objeto, como objetos de nó, nó folha, nó de política e nó de índice	Leitura	directory*		
ListObjectParents	Concede permissão para listar objetos pai associados a um determinado objeto em forma de paginação	Leitura	directory*		
ListObjectPolicies	Concede permissão para retornar as políticas anexadas a um objeto em forma de paginação	Leitura	directory*		
ListOutgoingTypedLinks	Concede permissão para retornar uma lista paginada de todas as saídas de um determinado TypedLinks objeto	Leitura	directory*		
ListPolicyAttachments	Concede permissão para devolver todas as informaçõ es ObjectIdentifiers às quais uma determinada política está anexada	Leitura	directory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListPublishedSchemaArns	Concede permissão para recuperar o esquema publicado ARNs	Lista			
ListTagsForResource	Concede permissão para retornar etiquetas de um recurso	Leitura	directory*		
ListTypedLinkFacetAttributes	Concede permissão para retornar uma lista paginada de atributos associados à faceta de link com tipo	Leitura	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
ListTypedLinkFacetNames	Concede permissão para retorna uma lista paginada de nomes de facetas de link com tipo existentes em um esquema	Leitura	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
LookupPolicy	Concede permissão para listar todas as políticas a partir da raiz do diretório para o objeto especificado	Leitura	directory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PublishSchema	Concede permissão para publicar um esquema de desenvolvimento com uma versão	Gravar	developmentSchema*		
PutSchemaFromJson	Concede permissão para atualizar um esquema usando o upload do JSON. Disponível apenas para esquemas de desenvolvimento	Gravar			
RemoveFacetFromObject	Concede permissão para remover a faceta especificada do objeto especificado	Gravar	directory*		
TagResource	Concede permissão para adicionar tags a um recurso	Marcação	directory*		
UntagResource	Concede permissão para remover etiquetas de um recurso	Tags	directory*		
UpdateFacet	Concede permissão aos atributos, regras ou ObjectType de uma faceta add/update/delete existentes	Gravar	appliedSchema*		
			developmentSchema*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateLinkAttributes	Concede permissão para atualizar os atributos de um determinado link digitado. Os atributos a serem atualizados não devem contribuir para a identidade do link digitado, conforme definido por seu IdentityAttributeOrder	Gravar	directory*		
UpdateObjectAttributes	Concede permissão para atualizar os atributos de um determinado objeto	Gravar	directory*		
UpdateSchema	Concede permissão para atualizar o nome do esquema com um novo nome	Gravar	developmentSchema*		
UpdateTypedLinkFacet	Concede permissão aos atributos, regras e ordem de atributos de identidade add/update/delete existentes de uma TypedLink faceta	Gravar	developmentSchema*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpgradeAppliedSchema	Concede permissão para atualizar um único diretório local usando as atualizações PublishedSchemaArn de esquema encontradas em. MinorVersion Atualizações de versões secundárias compatíveis com versões anteriores ficam instantaneamente disponíveis para leitores em todos os objetos no diretório	Gravar	directory*		
			publishedSchema*		
UpgradePublishedSchema	Concede permissão para atualizar um esquema publicado sob uma nova revisão de versão secundária usando o conteúdo atual do DevelopmentSchemaArn	Gravar	developmentSchema*		
			publishedSchema*		

Tipos de recursos definidos pelo Amazon Cloud Directory

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}`	
publishedSchema	`arn:${Partition}:clouddirectory:${Region}:${Account}:schema/published/${SchemaName}/${Version}`	

Chaves de condição do Amazon Cloud Directory

O Cloud Directory não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do Nuvem AWS Map

Nuvem AWS O mapa (prefixo do serviço:`servicediscovery`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Nuvem AWS Map
- Tipos de recursos definidos pelo Nuvem AWS Map
- Chaves de condição do Nuvem AWS Map

Ações definidas pelo Nuvem AWS Map

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateHttpNamespace	Concede permissão para criar um namespace HTTP	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreatePrivateDnsNamespace	Concede permissão para criar um namespace privado baseado no DNS, que será visível somente dentro de uma Amazon VPC especificada	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreatePublicDnsNamespace	Concede permissão para criar um namespace público baseado no DNS, que será visível na Internet	Write		aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateService	Concede permissão para criar um serviço	Write	namespace*		
			service*		
				servicediscovery:NamespaceArn aws:TagKeys aws:RequestTag/${TagKey}	
DeleteNamespace	Concede permissão para excluir um namespace especificado	Gravar	namespace*		
DeleteResourcePolicy [somente permissão]	Concede permissão para excluir a política de controle de acesso à RAM para um namespace	Gravar	namespace*		
DeleteService	Concede permissão para excluir um serviço especificado	Gravar	service*		
				servicediscovery:ServiceCreatedByAccount	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteServiceAttributes	Concede permissão para excluir atributos especificados de um serviço	Gravar	service*		
				servicediscovery:ServiceCreatedByAccount	
DeregisterInstance	Concede permissão para excluir os registros e a verificação de integridade, se houver, que o Amazon Route 53 criou para a instância especificada	Write	service*		
				servicediscovery:ServiceArn servicediscovery:ServiceCreatedByAccount	
DiscoverInstances	Concede permissão para descobrir instâncias registradas para um namespace e serviço especificados	Leitura	namespace*		
			service*		
				servicediscovery:NamespaceName servicediscovery:ServiceName	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DiscoverInstancesRevision	Concede permissão para descobrir a revisão de instâncias para um namespace e serviço especificados	Leitura	namespace*		
			service*		
				servicediscovery:NamespaceName servicediscovery:ServiceName	
GetInstance	Concede permissão para obter informações sobre uma instância especificada	Read	service*		
				servicediscovery:ServiceArn	
GetInstancesHealthStatus	Concede permissão para obter o status de integrida de atual (Saudável, Não Saudável ou Desconhecido) de uma ou mais instâncias	Read	service*		
				servicediscovery:ServiceArn	
GetNamespace	Concede permissão para obter informações sobre um namespace	Read	namespace*		
GetOperation	Concede permissão para obter informações sobre uma operação específica	Leitura	namespace*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			service		
GetResourcePolicy [somente permissão]	Concede permissão para ler a política de controle de acesso à RAM para um namespace	Leitura	namespace*		
GetService	Concede permissão para obter as configurações de um serviço especificado	Leitura	service*		
GetServiceAttributes	Concede permissão para obter os atributos de um serviço específico	Leitura	service*		
ListInstances	Concede permissão para obter informações resumidas sobre as instâncias que foram registradas em um serviço especificado	Leitura	service*		
				servicediscovery:ServiceArn	
ListNamespaces	Concede permissão para obter informações sobre os espaços de nome	Leitura			
ListOperations	Concede permissão para listar operações que correspondam aos critérios especificados	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListServices	Concede permissão para obter configurações para todos os serviços que correspondem aos filtros especificados	Leitura			
ListTagsForResource	Concede permissão para listas de etiquetas para o recurso especificado	Leitura			
PutResourcePolicy [somente permissão]	Concede permissão para definir a política de controle de acesso à RAM para um namespace	Gravar	namespace*		
RegisterInstance	Concede permissão para registrar uma instância com base nas configurações de um serviço especificado	Write	service*		
				servicediscovery:ServiceArn servicediscovery:ServiceCreatedByAccount	
TagResource	Concede permissão para adicionar uma ou mais etiquetas ao recurso especificado	Marcação		aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para remover uma ou mais etiquetas do recurso especificado	Tags		aws:TagKeys	
UpdateHttpNamespace	Concede permissão para atualizar as configurações de um namespace HTTP	Gravar	namespace*		
UpdateInstanceCustomHealthStatus	Concede permissão para atualizar o status de integridade atual para uma instância que tenha uma verificação de integridade personalizada	Gravar	service*		
				servicediscovery:ServiceArn servicediscovery:ServiceCreatedByAccount	
UpdatePrivateDnsNamespace	Concede permissão para atualizar as configurações de um namespace de DNS privado	Gravar	namespace*		
UpdatePublicDnsNamespace	Concede permissão para atualizar as configurações de um namespace de DNS público	Gravar	namespace*		
UpdateService	Concede permissão para atualizar as configurações em um serviço especificado	Gravar	service*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				servicediscovery:ServiceCreatedByAccount	
UpdateServiceAttributes	Concede permissão para atualizar os atributos em um serviço especificado	Gravar	service*		
				servicediscovery:ServiceCreatedByAccount	

Tipos de recursos definidos pelo Nuvem AWS Map

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
namespace	`arn:${Partition}:servicediscovery:${Region}:${Account}:namespace/${NamespaceId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
service	`arn:${Partition}:servicediscovery:${Region}:${Account}:service/${ServiceId}`	aws:ResourceTag/${TagKey}

Chaves de condição do Nuvem AWS Map

Nuvem AWS O mapa define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra ações com base nas etiquetas transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra as ações com base nas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra ações com base nas chaves da etiqueta transmitidas na solicitação	ArrayOfString
servicediscovery:NamespaceArn	Filtra o acesso especificando o Nome de recurso da Amazon (ARN) para o namespace relacionado	ARN
servicediscovery:NamespaceName	Filtra o acesso especificando o nome do namespace relacionado	String

Chaves de condição	Descrição	Tipo
servicediscovery:ServiceArn	Filtra o acesso especificando o Nome de recurso da Amazon (ARN) para o serviço relacionado	ARN
servicediscovery:ServiceCreatedByAccount	Filtra o acesso especificando o ID da conta do criador do serviço relacionado	String
servicediscovery:ServiceName	Filtra o acesso especificando o nome do serviço relacionado	String

Ações, recursos e chaves de condição do AWS Cloud9

AWS O Cloud9 (prefixo do serviço`cloud9`:) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Cloud9
- Tipos de recursos definidos pelo AWS Cloud9
- Chaves de condição do AWS Cloud9

Ações definidas pelo AWS Cloud9

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando

usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ActivateEC2Remote [somente permissão]	Concede permissão para iniciar a EC2 instância da Amazon à qual seu AWS Cloud9 IDE se conecta	Gravar	environment*		
CreateEnvironmentEC2	Concede permissão para criar um AWS ambiente de desenvolvimento Cloud9, lança uma instância do Amazon Elastic Compute Cloud (EC2Amazon) e, em seguida, hospeda o ambiente na instância	Gravar		cloud9:EnvironmentName cloud9:InstanceType cloud9:SubnetId cloud9:UserArn cloud9:OwnerArn aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole
CreateEnvironmentMembership	Concede permissão para adicionar um membro do ambiente a um ambiente de desenvolvimento do AWS Cloud9	Gravar	environment*		
				cloud9:UserArn	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				cloud9:EnvironmentId cloud9:Permissions	
CreateEnvironmentSSH [somente permissão]	Concede permissão para criar um ambiente de desenvolvimento AWS Cloud9 SSH	Gravar		cloud9:EnvironmentName cloud9:OwnerArn aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironmentToken [somente permissão]	Concede permissão para criar um token de autenticação que permite uma conexão entre o AWS Cloud9 IDE e o ambiente do usuário	Leitura	environment*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteEnvironment	Concede permissão para excluir um ambiente de desenvolvimento do AWS Cloud9. Se o ambiente estiver hospedado em uma instância do Amazon Elastic Compute Cloud (Amazon EC2), a instância também será encerrada	Gravar	environment*		iam:CreateServiceLinkedRole
DeleteEnvironmentMembership	Concede permissão para excluir um membro do ambiente de um ambiente de desenvolvimento do AWS Cloud9	Gravar	environment*		
				cloud9:UserArn cloud9:EnvironmentId	
DescribeEC2Remote [somente permissão]	Concede permissão para obter detalhes sobre a conexão com o ambiente de EC2 desenvolvimento, incluindo host, usuário e porta	Leitura	environment*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeEnvironmentMemberships	Concede permissão para obter informações sobre membros do ambiente para um ambiente de desenvolvimento AWS Cloud9	Leitura	environment*		
				cloud9:UserArn cloud9:EnvironmentId	
DescribeEnvironmentStatus	Concede permissão para obter informações de status para um ambiente de desenvolvimento do AWS Cloud9	Leitura	environment*		
DescribeEnvironments	Concede permissão para obter informações sobre os ambientes de desenvolvimento do AWS Cloud9	Leitura	environment*		
DescribeSSHRemote [somente permissão]	Concede permissão para obter detalhes sobre a conexão com o ambiente de desenvolvimento SSH, incluindo host, usuário e porta	Leitura	environment*		
GetEnvironmentConfig [somente permissão]	Concede permissão para obter informações de configuração usadas para inicializar o IDE AWS Cloud9	Leitura	environment*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetEnvironmentSettings [somente permissão]	Concede permissão para obter as configurações do AWS Cloud9 IDE para um ambiente de desenvolvimento específico	Leitura	environment*		
GetMembershipSettings [somente permissão]	Concede permissão para obter as configurações do AWS Cloud9 IDE para um membro do ambiente especificado	Leitura	environment*		
GetMigrationExperiences [somente permissão]	Concede permissão para obter a experiência de migração para um usuário do cloud9	Leitura			
GetUserPublicKey [somente permissão]	Concede permissão para obter a chave SSH pública do usuário, que é usada pelo AWS Cloud9 para se conectar aos ambientes de desenvolvimento SSH	Leitura		cloud9:UserArn	
GetUserSettings [somente permissão]	Concede permissão para obter as configurações do AWS Cloud9 IDE para um usuário especificado	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListEnvironments	Concede permissão para obter uma lista de identificadores do ambiente de AWS desenvolvimento do Cloud9	Leitura			
ListTagsForResource	Concede permissão para listar as etiquetas para um ambiente do cloud9	Leitura	environment*		
ModifyTemporaryCredentialsOnEnvironmentEC2 [somente permissão]	Concede permissão para definir credenciais temporárias AWS gerenciadas na EC2 instância da Amazon que é usada pelo ambiente de desenvolvimento integrado AWS (IDE) Cloud9	Gravar	environment*		
TagResource	Concede permissão para adicionar as etiquetas ao ambiente do cloud9	Tags	environment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover as etiquetas ao ambiente do cloud9	Tags	environment*		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateEnvironment	Concede permissão para alterar as configurações de um ambiente de desenvolvimento existente do AWS Cloud9	Gravar	environment*		
UpdateEnvironmentMembership	Concede permissão para alterar as configurações de um membro do ambiente existente para um ambiente de desenvolvimento AWS Cloud9	Gravar	environment*		
				cloud9:UserArn cloud9:EnvironmentId cloud9:Permissions	
UpdateEnvironmentSettings [somente permissão]	Concede permissão para atualizar as configurações do AWS Cloud9 IDE para um ambiente de desenvolvimento especificado	Gravar	environment*		
UpdateMembershipSettings [somente permissão]	Concede permissão para atualizar as configurações do AWS Cloud9 IDE para um membro do ambiente especificado	Gravar	environment*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateSSHRemote [somente permissão]	Concede permissão para atualizar os detalhes sobre a conexão com o ambiente de desenvolvimento SSH, incluindo host, usuário e porta	Gravar	environment*		
UpdateUserSettings [somente permissão]	Concede permissão para atualizar as configurações específicas do IDE de um usuário do Cloud9 AWS	Gravar			

Tipos de recursos definidos pelo AWS Cloud9

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
environment	`arn:${Partition}:cloud9:${Region}:${Account}:environment:${ResourceId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Cloud9

AWS O Cloud9 define as seguintes chaves de condição que podem ser usadas no elemento de uma `Condition` política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob

as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString
cloud9:EnvironmentId	Filtra o acesso pelo ID do AWS ambiente Cloud9	String
cloud9:EnvironmentName	Filtra o acesso pelo nome do AWS ambiente Cloud9	String
cloud9:InstanceType	Filtra o acesso pelo tipo de instância da instância Amazon do ambiente AWS Cloud9 EC2	String
cloud9:OwnerArn	Filtra o acesso pelo ARN do proprietário especificado	ARN
cloud9:Permissions	Filtra o acesso pelo tipo de permissões do AWS Cloud9	String
cloud9:SubnetId	Filtra o acesso pelo ID da sub-rede em que o AWS ambiente Cloud9 será criado	String
cloud9:UserArn	Filtra o acesso pelo ARN do usuário especificado	ARN

Ações, recursos e chaves de condição para o AWS CloudFormation

AWS CloudFormation (prefixo do serviço:`cloudformation`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS CloudFormation
- Tipos de recursos definidos pelo AWS CloudFormation
- Chaves de condição do AWS CloudFormation

Ações definidas pelo AWS CloudFormation

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ActivateOrganizationsAccess	Concede permissão para ativar o acesso confiável entre StackSets e Organizations. Com o acesso confiável entre StackSets e Organizations ativado, a conta de gerenciamento tem permissões StackSets para criar e gerenciar sua organização	Gravar			
ActivateType	Concede permissão para ativar uma extensão pública de terceiros, tornando-a	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	disponível para uso em modelos de pilha				
BatchDescribeTypeConfigurations	Concede permissão para retornar dados de configuração para as CloudFormation extensões especificadas	Leitura			
CancelUpdateStack	Concede permissão para cancelar uma atualização na pilha especificada	Write	stack*		
ContinueUpdateRollback	Concede permissão para continuar revertendo uma pilha que está no estado UPDATE_ROLLBACK_FAILED para o estado UPDATE_ROLLBACK_COMPLETE	Write	stack*		
				cloudformation:RoleArn	
CreateChangeSet	Concede permissão para criar uma lista de alterações para uma pilha	Gravar	stack*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				cloudformation:ChangeSetName cloudformation:ResourceTypes cloudformation:ImportResourceTypes cloudformation:RoleArn cloudformation:StackPolicyUrl cloudformation:TemplateUrl aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
CreateGeneratedTemplate	Concede permissão para criar um modelo a partir de recursos existentes que ainda não foram gerenciados com CloudFormation	Gravar			
CreateStack	Concede permissão para criar uma pilha conforme especificado no modelo	Write	stack*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				cloudformation:ResourceTypes cloudformation:RoleArn cloudformation:StackPolicyUrl cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	
CreateStackInstances	Concede permissão para criar instâncias de pilha para as contas especificadas, dentro das regiões especificadas	Gravar	stackset*		
			stackset-target		
			type		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys cloudformation:TargetRegion	
CreateStackRefactor	Concede permissão para criar uma refatoração de pilha	Gravar	stack*		
CreateStackSet	Concede permissão para criar um conjunto de pilha conforme especificado no modelo	Write		cloudformation:RoleArn cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	
CreateUploadBucket [somente permissão]	Concede permissão para enviar modelos para buckets do Amazon S3. Usado somente pelo AWS CloudFormation console e não está documentado na referência da API	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeactivateOrganizationsAccess	Concede permissão para desativar o acesso confiável entre StackSets e Organizations. Se o acesso confiável for desativado, a conta de gerenciamento não terá permissões para criar e gerenciar serviços gerenciados StackSets para sua organização	Gravar			
DeactivateType	Concede permissão para desativar uma extensão pública que foi ativada anteriormente nesta conta e região	Gravar			
DeleteChangeSet	Concede permissão para excluir o conjunto de alterações especificado. A exclusão de conjuntos de alterações garante que ninguém execute o conjunto de alterações errado	Gravar	stack*		
				cloudformation:ChangeSetName	
DeleteGeneratedTemplate	Concede permissão para excluir um modelo gerado	Gravar			
DeleteStack	Concede permissão para excluir uma pilha especificada	Write	stack*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				cloudformation:RoleArn	
DeleteStackInstances	Concede permissão para excluir instâncias de pilha para as contas especificadas, nas regiões especificadas	Write	stackset*		
			stackset-target		
			type		
				cloudformation:TargetRegion	
DeleteStackSet	Concede permissão para excluir um conjunto de pilha especificado	Gravar	stackset*		
DeregisterType	Concede permissão para cancelar o registro de um CloudFormation tipo ou versão de tipo existente	Gravar			
DescribeAccountLimits	Concede permissão para recuperar os limites da AWS CloudFormation sua conta	Leitura			
DescribeChangeSet	Concede permissão para devolver a descrição do conjunto de alterações especificado	Leitura	stack*		
				cloudformation:ChangeSetName	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeChangeSetHooks	Concede permissão para devolver as informações da chamada do Hook para o conjunto de alterações especificado	Leitura	stack*		
				cloudformation:ChangeSetName	
DescribeGeneratedTemplate	Concede permissão para descrever um modelo gerado. A saída inclui detalhes sobre o progresso da criação de um modelo gerado	Leitura			
DescribeOrganizationsAccess	Concede permissão para retornar informações sobre o OrganizationAccess status da conta	Leitura			
DescribePublisher	Concede permissão para devolver informações sobre um editor CloudFormation de extensões	Leitura			
DescribeResourceScan	Concede permissão para descrever detalhes de uma verificação de recursos	Leitura			
DescribeStackDriftDetectionStatus	Concede permissão para devolver informações sobre uma operação de detecção de desvio de pilha	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeStackEvents	Concede permissão para devolver todos os eventos relacionados à pilha para uma pilha especificada	Leitura	stack*		
DescribeStackInstance	Concede permissão para retornar a instância da pilha associada ao conjunto de pilhas e à região especificados Conta da AWS	Leitura	stackset*		
DescribeStackRefactor	Concede permissão para retornar a descrição do refator de pilha especificado	Leitura	stack*		
DescribeStackResource	Concede permissão para devolver uma descrição do recurso especificado na pilha especificada	Read	stack*		
DescribeStackResourceDrifts	Concede permissão para retornar informações de desvio para os recursos que foram verificados quanto ao desvio na pilha especificada	Leitura	stack*		
DescribeStackResources	Concede permissão para retornar descrições AWS de recursos para pilhas em execução e excluídas	Leitura	stack*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeStackSet	Concede permissão para devolver a descrição do conjunto de pilha especificado	Read	stackset*		
DescribeStackSetOperation	Concede permissão para devolver a descrição da operação de conjunto de pilha especificada	Leitura	stackset*		
DescribeStacks	Concede permissão para retornar a descrição da pilha especificada e de todas as pilhas quando usada em combinação com a ação ListStacks	Lista	stack		cloudformation:ListStacks
DescribeType	Concede permissão para retornar informações sobre o CloudFormation tipo solicitado	Leitura			
DescribeTypeRegistration	Concede permissão para retornar informações sobre o processo de registro de um CloudFormation tipo	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DetectStackDrift	Concede permissão para detectar se a configuração real de uma pilha difere, ou foi derivada, da configuração esperada, conforme definido no modelo de pilha e quaisquer valores especificados como parâmetros de modelo	Read	stack*		
DetectStackResourceDrift	Concede permissão para retornar informações sobre se a configuração real de um recurso difere ou se foi derivada da configuração esperada, conforme definido no modelo de pilha e quaisquer valores especificados como parâmetros de modelo	Read	stack*		
DetectStackSetDrift	Concede permissão para permitir que os usuários detectem desvio em um conjunto de pilha e as instâncias de pilha que pertencem a esse conjunto de pilhas	Read	stackset*		
EstimateTemplateCost	Concede permissão para devolver o custo mensal estimado de um modelo	Read		cloudformation:TemplateUrl	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ExecuteChangeSet	Concede permissão para atualizar uma pilha usando as informações de entrada fornecidas quando o conjunto de alterações especificado foi criado	Gravar	stack*		
				cloudformation:ChangeSetName	
ExecuteStackRefactor	Concede permissão para executar uma refatoração de pilha usando as informações de entrada fornecidas quando a refatoração de pilha especificada foi criada	Gravar	stack*		
GetGeneratedTemplate	Concede permissão para recuperar um modelo gerado	Leitura			
GetStackPolicy	Concede permissão para devolver a política de pilha para uma pilha especificada	Read	stack*		
GetTemplate	Concede permissão para devolver o corpo do modelo para uma pilha especificada	Read	stack*		
GetTemplateSummary	Concede permissão para devolver informações sobre um modelo novo ou existente	Leitura	stack		
			stackset		
				cloudformation:TemplateUrl	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ImportStacksToStackSet	Concede permissão para permitir que os usuários importem pilhas existentes para um conjunto de pilhas novo ou existente	Gravar	stackset*		
ListChangeSets	Concede permissão para devolver a ID e o status de cada conjunto de alterações ativas para uma pilha. Por exemplo, AWS CloudFormation lista os conjuntos de alteraçõe s que estão no estado CREATE_IN_PROGRESS ou CREATE_PENDING	Lista	stack*		
ListExports	Concede permissão para listar todos os valores de saída exportados na conta e região em que você chama essa ação	Lista			
ListGeneratedTemplates	Concede permissão para listar seus modelos gerados nessa região	Lista			
ListHookResults	Concede permissão para retornar as informações do resultado das invocações de Hook para o destino especificado	Lista	stack		
				cloudformation:ChangeSetName	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListImports	Concede permissão para listar todas as pilhas que estão importando um valor de saída exportado	Lista			
ListResourceScanRelatedResources	Concede permissão para listar os recursos relacionados para obter uma lista de recursos usando uma verificação de recursos. A resposta indica se cada recurso retornado já é gerenciado pelo CloudFormation	Lista			
ListResourceScanResources	Concede permissão para listar os recursos usando uma verificação de recursos. Os resultados podem ser filtrados por identificador de recurso, prefixo do tipo de recurso, chave da tag e valor da tag	Lista			
ListResourceScans	Concede permissão para listar as verificações de recursos da mais recente para a mais antiga. Por padrão, retornará até 10 verificações de recursos	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListStackInstanceResourceDrifts	Concede permissão para retornar informações de desvio para os recursos que foram verificados quanto ao desvio na instância da pilha especificada	Lista	stackset*		
ListStackInstances	Concede permissão para devolver informações de resumo sobre instâncias de pilha associadas ao conjunto de pilha especificado	Lista	stackset*		
ListStackRefactorActions	Concede permissão para retornar a lista de ações do refator de pilha especificado	Lista	stack*		
ListStackRefactors	Concede permissão para retornar o ID e o status de cada refator de pilha ativo	Lista	stack*		
ListStackResources	Concede permissão para devolver descrições de todos os recursos da pilha especificada	Lista	stack*		
ListStackSetAutoDeploymentTargets	Concede permissão para retornar informações resumidas sobre metas de implantação StackSet automática	Lista	stackset*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListStackSetOperationResults	Concede permissão para devolver informações resumidas sobre os resultados de uma operação de conjunto de pilha	List	stackset*		
ListStackSetOperations	Concede permissão para devolver informações resumidas sobre operações executadas em um conjunto de pilhas	List	stackset*		
ListStackSets	Concede permissão para devolver informações de resumo sobre conjuntos de pilha associados ao usuário	Lista			
ListStacks	Concede permissão para retornar as informações resumidas das pilhas cujo status corresponda ao especificado StackStatusFilter. Em combinação com a DescribeStacks ação, concede permissão para listar as descrições das pilhas	Lista			
ListTypeRegistrations	Concede permissão para listar tentativas CloudFormation de registro do tipo	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTypeVersions	Concede permissão para listar versões de um CloudFormation tipo específico	Lista			
ListTypes	Concede permissão para listar CloudFormation os tipos disponíveis	Lista			
PublishType	Concede permissão para publicar a extensão especificada no CloudFormation registro como uma extensão pública nesta região	Gravar			
RecordHandlerProgress	Concede permissão para registrar o progresso do manipulador	Gravar	stack*		
RegisterPublisher	Concede permissão para registrar uma conta como editora de extensões públicas no CloudFormation registro	Gravar			
RegisterType	Concede permissão para registrar um novo CloudFormation tipo	Gravar			
RollbackStack	Concede permissão para reverter a pilha ao último estado estável	Gravar	stack*		
				cloudformation:RoleArn	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SetStackPolicy	Concede permissão para definir uma política de pilha para uma pilha especificada	Gerenciamento de permissões	stack*		
				cloudformation:StackPolicyUrl	
SetTypeConfiguration	Concede permissão para definir os dados de configuração de uma CloudFormation extensão registrada, em determinada conta e região	Gravar			
SetTypeDefaultVersion	Concede permissão para definir qual versão de um CloudFormation tipo se aplica às CloudFormation operações	Gravar			
SignalResource	Concede permissão para enviar um sinal para o recurso especificado com um status de sucesso ou falha	Gravar	stack*		
StartResourceScan	Concede permissão para iniciar uma verificação dos recursos da conta nessa região	Gravar			
StopStackSetOperation	Concede permissão para interromper uma operação em andamento em um conjunto de pilha e suas instâncias de pilha associadas	Write	stackset*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para marcar recursos do cloudformation	Tags	changeset		
			stack		
			stackset		
				aws:TagKeys aws:RequestTag/${TagKey} cloudformation:CreateAction	
TestType	Concede permissão para testar uma extensão registrada para garantir que ela atenda a todos os requisitos necessários para ser publicada no CloudFormation registro	Gravar			
UntagResource	Concede permissão para desmarcar recursos do cloudformation	Tags	changeset		
			stack		
			stackset		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys cloudformation:CreateAction	
UpdateGeneratedTemplate	Concede permissão para atualizar um modelo gerado. Isso pode ser usado para alterar o nome, adicionar e remover recursos, atualizar recursos e alterar as configurações DeletionPolicy e. UpdateReplacePolicy	Gravar			
UpdateStack	Concede permissão para atualizar uma pilha conforme especificado no modelo	Write	stack*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				cloudformation:ResourceTypes cloudformation:RoleArn cloudformation:StackPolicyUrl cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	
UpdateStackInstances	Concede permissão para atualizar os valores de parâmetro para instâncias de pilha para as contas especificadas, dentro das regiões especificadas	Write	stackset*		
			stackset-target		
			type		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				cloudformation:TargetRegion	
UpdateStackSet	Concede permissão para atualizar um conjunto de pilha conforme especificado no modelo	Write	stackset*		
			stackset-target		
			type		
				cloudformation:RoleArn cloudformation:TemplateUrl cloudformation:TargetRegion aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTerminationProtection	Concede permissão para atualizar a proteção de encerramento para a pilha especificada	Write	stack*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ValidateTemplate	Concede permissão para validar um modelo especificado	Leitura		cloudformation:TemplateUrl	

Tipos de recursos definidos pelo AWS CloudFormation

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
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}`	

Chaves de condição do AWS CloudFormation

AWS CloudFormation define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Chaves de condição	Descrição	Tipo
cloudformation:ChangeSetName	Filtra o acesso pelo nome do conjunto de AWS CloudFormation alterações. Use para controlar quais conjuntos de alterações os usuários do IAM podem executar ou excluir	String
cloudformation:CreateAction	Filtra o acesso pelo nome de uma ação de API que altera o recurso. Use para controlar quais usuários APIs do IAM podem usar para adicionar ou remover tags em uma pilha ou conjunto de pilhas	String
cloudformation:ImportResourceTypes	Filtra o acesso pelos tipos de recursos do modelo, como AWS::EC2: :Instance. Use para controlar com quais tipos de recursos os usuários do IAM podem trabalhar quando quiserem importar um recurso para uma pilha	String
cloudformation:ResourceTypes	Filtra o acesso pelos tipos de recursos do modelo, como AWS::EC2: :Instance. Use para controlar com quais tipos de recursos os usuários do IAM podem trabalhar ao criar ou atualizar uma pilha	ArrayOfString
cloudformation:RoleArn	Filtra o acesso por ARN de uma função de serviço do IAM. Use para controlar qual função de serviço os usuários do IAM podem usar para trabalhar com pilhas ou conjuntos de alterações	ARN
cloudformation:StackPolicyUrl	Filtra o acesso por um URL de política de pilha do Amazon S3. Use para controlar quais políticas de pilha os usuários do IAM podem associar a uma pilha durante uma ação de criação ou atualização	String
cloudformation:TargetRegion	Filtra o acesso por região de destino do conjunto de pilhas. Use para controlar quais regiões os usuários do IAM podem usar quando criam ou atualizam conjuntos de pilhas	ArrayOfString

Chaves de condição	Descrição	Tipo
cloudformation:TemplateUrl	Filtra o acesso por um URL de modelo do Amazon S3. Use para controlar quais modelos os usuários do IAM podem usar quando criam ou atualizam pilhas	String

Ações, recursos e chaves de condição para a Amazon CloudFront

A Amazon CloudFront (prefixo do serviço:`cloudfront`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon CloudFront
- Tipos de recursos definidos pela Amazon CloudFront
- Chaves de condição para a Amazon CloudFront

Ações definidas pela Amazon CloudFront

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AllowVendedLogDeliveryForResource	Concede permissão para configurar a entrega de registros vendidos para uma distribuição	Gerenciamento de permissões	distribution		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
[somente permissão]					
AssociateAlias	Concede permissão para associar um alias a uma distribuição CloudFront	Gravar	distribution*		
AssociateDistributionTenantWebACL	Concede permissão para associar um inquilino de distribuição a uma ACL web do AWS WAF	Gravar	distribution-tenant*		
AssociateDistributionWebACL	Concede permissão para associar uma distribuição a uma Web ACL AWS do WAF	Gravar	distribution*		
CopyDistribution	Concede permissão para copiar uma distribuição existente e criar uma nova distribuição na web	Gravar	distribution*		cloudfront:CopyDistribution cloudfront:CreateDistribution cloudfront:GetDistribution
CreateAnycastIpList	Concede permissão para criar uma lista de IPs estáticos Anycast	Gravar	anycast-ip-list*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCachePolicy	Concede permissão para adicionar uma nova política de cache ao CloudFront	Gravar	cache-policy*		
CreateCloudFrontOriginAccessIdentity	Concede permissão para criar uma nova identidade de acesso de CloudFront origem	Gravar	origin-access-identity*		
CreateConnectionGroup	Concede permissão para criar um grupo de conexão	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateContinuousDeploymentPolicy	Concede permissão para adicionar uma nova política de implantação contínua ao CloudFront	Gravar	continuous-deployment-policy*		
CreateDistribution	Concede permissão para criar uma nova distribuição na Web	Gravar	distribution*		cloudfront:CreateConnectionGroup

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDistributionTenant	Concede permissão para criar um inquilino de distribuição	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFieldLevelEncryptionConfig	Concede permissão para criar uma nova configuração de criptografia em nível de campo	Write			
CreateFieldLevelEncryptionProfile	Concede permissão para criar um perfil de criptografia em nível de campo	Gravar			
CreateFunction	Concede permissão para criar uma CloudFront função	Gravar	function*		
CreateInvalidation	Concede permissão para criar uma nova solicitação de lote de invalidação	Gravar	distribution*		
CreateInvalidationForDistributionTenant	Concede permissão para criar uma invalidação para um inquilino de distribuição	Gravar	distribution-tenant*		
CreateKeyGroup	Concede permissão para adicionar um novo grupo de chaves ao CloudFront	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateKeyValueStore	Concede permissão para criar um CloudFront KeyValueStore	Gravar	key-value-store*		
CreateMonitoringSubscription	Concede permissão para ativar CloudWatch métricas adicionais para a CloudFront distribuição especificada. As métricas adicionais incorrem em um custo adicional	Gravar			
CreateOriginAccessControl	Concede permissões para criar um novo controle de acesso de origem	Gravar			
CreateOriginRequestPolicy	Concede permissão para adicionar uma nova política de solicitação de origem ao CloudFront	Gravar	origin-request-policy*		
CreatePublicKey	Concede permissão para adicionar uma nova chave pública ao CloudFront	Gravar			
CreateRealtimeLogConfig	Concede permissão para criar uma configuração de log em tempo real	Gravar	realtime-log-config*		
CreateResponseHeadersPolicy	Concede permissão para adicionar uma nova política de cabeçalhos de resposta ao CloudFront	Gravar	response-headers-policy*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSavingsPlan [somente permissão]	Concede permissão para criar um novo savings plan	Gravar			
CreateStreamingDistribution	Concede permissão para criar uma nova distribuição RMTP	Write	streaming-distribution*		
CreateStreamingDistributionWithTags	Concede permissão para criar uma nova distribuição RMTP com etiquetas	Gravar	streaming-distribution*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVpcOrigin	Concede permissão para criar uma origem de VPC	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAnycastIpList	Concede permissão para excluir uma lista de IPs estáticos do Anycast	Gravar	anycast-ip-list*		
DeleteCachePolicy	Concede permissão para excluir uma política de cache	Gravar	cache-policy*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteCloudFrontOriginAccessIdentity	Concede permissão para excluir uma identidade de acesso de CloudFront origem	Gravar	origin-access-identity*		
DeleteConnectionGroup	Concede permissão para excluir um grupo de conexão	Gravar	connection-group*		
DeleteContinuousDeploymentPolicy	Concede permissão para excluir uma política de implantação contínua	Gravar	continuous-deployment-policy*		
DeleteDistribution	Concede permissão para excluir uma distribuição da Web	Gravar	distribution*		
DeleteDistributionTenant	Concede permissão para excluir um inquilino de distribuição	Gravar	distribution-tenant*		
DeleteFieldLevelEncryptionConfig	Concede permissão para excluir uma configuração de criptografia em nível de campo	Write	field-level-encryption-config*		
DeleteFieldLevelEncryptionProfile	Concede permissão para excluir um perfil de criptografia em nível de campo	Gravar	field-level-encryption-profile*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteFunction	Concede permissão para excluir uma CloudFront função	Gravar	function*		
DeleteKeyGroup	Concede permissão para excluir um grupo de chaves	Gravar			
DeleteKeyValueStore	Concede permissão para excluir um CloudFront KeyValueStore	Gravar	key-value-store*		
DeleteMonitoringSubscription	Concede permissão para desativar CloudWatch métricas adicionais para a CloudFront distribuição especificada	Gravar			
DeleteOriginAccessControl	Concede permissão para excluir um controle de acesso de origem	Gravar	origin-access-control*		
DeleteOriginRequestPolicy	Concede permissão para excluir uma política de solicitação de origem	Gravar	origin-request-policy*		
DeletePublicKey	Concede permissão para excluir uma chave pública do CloudFront	Gravar			
DeleteRealtimeLogConfig	Concede permissão para excluir uma configuração de log em tempo real	Gravar	realtime-log-config*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteResponseHeadersPolicy	Concede permissão para excluir uma política de cabeçalhos de resposta	Gravar	response-headers-policy*		
DeleteStreamingDistribution	Concede permissão para excluir uma distribuição RMTP	Gravar	streaming-distribution*		
DeleteVpcOrigin	Concede permissão para excluir uma origem de VPC	Gravar	vpcorigin*		
DescribeFunction	Concede permissão para obter um resumo CloudFront da função	Leitura	function*		
DescribeKeyValueStore	Concede permissão para obter um CloudFront KeyValueStore resumo	Leitura	key-value-store*		
DisassociateDistributionTenantWebACL	Concede permissão para desassociar um inquilino de distribuição de uma ACL web do AWS WAF	Gravar	distribution-tenant*		
DisassociateDistributionWebACL	Concede permissão para desassociar uma distribuição de uma ACL web do AWS WAF	Gravar	distribution*		
GetAnycastIpList	Concede permissão para obter uma lista de IPs estáticos do Anycast	Leitura	anycast-ip-list*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetCachePolicy	Concede permissão para obter a política de cache	Read	cache-policy*		
GetCachePolicyConfig	Concede permissão para obter a configuração da política de cache	Leitura	cache-policy*		
GetCloudFrontOriginAccessIdentity	Concede permissão para obter as informações sobre uma identidade de acesso de CloudFront origem	Leitura	origin-access-identity*		
GetCloudFrontOriginAccessIdentityConfig	Concede permissão para obter as informações de configuração sobre uma identidade do acesso de origem do CloudFront	Leitura	origin-access-identity*		
GetConnectionGroup	Concede permissão para obter informações sobre um grupo de conexão	Leitura	connection-group*		
GetConnectionGroupByRoutingEndpoint	Concede permissão para obter informações sobre um grupo de conexão pelo ponto final de roteamento especificado	Leitura	connection-group*		
GetContinuousDeploymentPolicy	Concede permissão para obter a política de implantação contínua	Leitura	continuous-deployment-policy*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetContinuousDeploymentPolicyConfig	Concede permissão para obter a configuração da política de implantação contínua	Leitura	continuous-deployment-policy*		
GetDistribution	Concede permissão para obter as informações sobre uma distribuição da Web	Read	distribution*		
GetDistributionConfig	Concede permissão para obter as informações de configuração de uma distribuição	Leitura	distribution*		
GetDistributionTenant	Concede permissão para obter informações sobre um inquilino de distribuição	Leitura	distribution-tenant*		
GetDistributionTenantByDomain	Concede permissão para obter informações sobre um locatário de distribuição pelo domínio associado	Leitura	distribution-tenant*		
GetFieldLevelEncryption	Concede permissão para obter as informações de configuração de criptografia em nível de campo	Read	field-level-encryption-config*		
GetFieldLevelEncryptionConfig	Concede permissão para obter as informações de configuração de criptografia em nível de campo	Read	field-level-encryption-config*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetFieldLevelEncryptionProfile	Concede permissão para obter as informações de configuração de criptografia em nível de campo	Read	field-level-encryption-profile*		
GetFieldLevelEncryptionProfileConfig	Concede permissão para obter as informações de configuração de perfil de criptografia em nível de campo	Leitura	field-level-encryption-profile*		
GetFunction	Concede permissão para obter o código de uma CloudFront função	Leitura	function*		
GetInvalidation	Concede permissão para obter as informações sobre uma invalidação	Leitura	distribution*		
GetInvalidationForDistributionTenant	Concede permissão para obter informações sobre uma invalidação para um inquilino de distribuição	Leitura	distribution-tenant*		
GetKeyGroup	Concede permissão para obter um grupo de chaves	Read			
GetKeyGroupConfig	Concede permissão para obter a configuração de um grupo de chaves	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetManagedCertificateDetails	Concede permissão para obter detalhes sobre um certificado CloudFront gerenciado	Leitura	distribution-tenant*		
GetMonitoringSubscription	Concede permissão para obter informações sobre se CloudWatch métricas adicionais estão habilitadas para a CloudFront distribuição especificada	Leitura			
GetOriginAccessControl	Concede permissão para obter o controle de acesso de origem	Leitura	origin-access-control*		
GetOriginAccessControlConfig	Concede permissão para obter a configuração do controle de acesso de origem	Leitura	origin-access-control*		
GetOriginRequestPolicy	Concede permissão para obter a política de solicitação de origem	Read	origin-request-policy*		
GetOriginRequestPolicyConfig	Concede permissão para obter a configuração da política de solicitação de origem	Read	origin-request-policy*		
GetPublicKey	Concede permissão para obter as informações da chave pública	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetPublicKeyConfig	Concede permissão para obter as informações de configuração da chave pública	Read			
GetRealtimeLogConfig	Concede permissão para obter uma configuração de log em tempo real	Leitura	realtime-log-config*		
GetResponseHeadersPolicy	Concede permissão para obter a política de cabeçalhos de resposta	Leitura	response-headers-policy*		
GetResponseHeadersPolicyConfig	Concede permissão para obter a configuração da política de cabeçalhos de resposta	Leitura	response-headers-policy*		
GetSavingsPlan [somente permissão]	Concede permissão para obter um savings plan	Leitura			
GetStreamingDistribution	Concede permissão para obter as informações sobre uma distribuição RMTP	Read	streaming-distribution*		
GetStreamingDistributionConfig	Concede permissão para obter as informações de configuração de uma distribuição de transmissão	Leitura	streaming-distribution*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetVpcOrigin	Concede permissão para obter as informações sobre uma origem de VPC	Leitura	vpcorigin*		
ListAnycastIpLists	Concede permissão para listar suas listas de IP estáticos do Anycast	Lista			
ListCachePolicies	Concede permissão para listar todas as políticas de cache que foram criadas CloudFront para essa conta	Lista			
ListCloudFrontOriginAccessIdentities	Concede permissão para listar suas identidades de acesso de CloudFront origem	Lista			
ListConflictingAliases	Concede permissão para listar todos os aliases que entram em conflito com o alias fornecido no CloudFront	Lista	distribution*		
ListConnectionGroups	Concede permissão para listar os grupos de conexão em seu Conta da AWS	Lista			
ListContinuousDeploymentPolicies	Concede permissão para listar todas as políticas de implantação contínua na conta	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDistributionTenants	Concede permissão para listar os inquilinos de distribuição em seu Conta da AWS	Lista			
ListDistributionTenantsByCustomization	Concede permissão para listar os inquilinos de distribuição pela personalização que você especificar	Lista			
ListDistributions	Concede permissão para listar as distribuições associadas à sua Conta da AWS	Lista			
ListDistributionsByAnycastIpListId	Concede permissão para listar as distribuições em sua conta que estão associadas ao especificado AnycastIp ListId	Lista			
ListDistributionsByCachePolicyId	Concede permissão para listar a distribuição IDs para distribuições que têm um comportamento de cache associado à política de cache especificada	Lista			
ListDistributionsByConnectionMode	Concede permissão para listar as distribuições pelo modo de conexão especificado	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDistributionsByKeyGroup	Concede permissão para listar a distribuição IDs para distribuições que têm um comportamento de cache associado ao grupo de chaves especificado	Lista			
ListDistributionsByLambdaFunction [somente permissão]	Concede permissão para listar todas as distribuições associadas a uma função do Lambda	Lista			
ListDistributionsByOriginRequestPolicyId	Concede permissão para listar a distribuição IDs para distribuições que têm um comportamento de cache associado à política de solicitação de origem especificada	Lista			
ListDistributionsByRealtimeLogConfig	Concede permissão para obter uma lista de distribuições que têm um comportamento de cache associado à configuração de log em tempo real especificada	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDistributionsByResponseHeadersPolicyId	Concede permissão para listar a distribuição IDs para distribuições que têm um comportamento de cache associado à política de cabeçalhos de resposta especificada	Lista			
ListDistributionsByVpcOriginId	Concede permissão IDs para listar distribuições associadas à origem da VPC especificada	Lista			
ListDistributionsByWebACLId	Concede permissão para listar as distribuições associadas à sua determinada ACL Conta da AWS web do AWS WAF	Lista			
ListDomainConflicts	Concede permissão para listar conflitos de domínio para um domínio especificado	Lista	distribution distribution-tenant		
ListFieldLevelEncryptionConfigs	Concede permissão para listar todas as configurações de criptografia em nível de campo que foram criadas para essa conta CloudFront	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListFieldLevelEncryptionProfiles	Concede permissão para listar todos os perfis de criptografia em nível de campo que foram criados CloudFront para essa conta	Lista			
ListFunctions	Concede permissão para obter uma lista de CloudFront funções	Lista			
ListInvalidations	Concede permissão para listar seus lotes de invalidação	Lista	distribution*		
ListInvalidationsForDistributionTenant	Concede permissão para listar as invalidações de um inquilino de distribuição	Lista	distribution-tenant*		
ListKeyGroups	Concede permissão para listar todos os grupos-chave que foram criados CloudFront para essa conta	Lista			
ListKeyValueStores	Concede permissão para obter uma lista de CloudFront KeyValueStores	Lista			
ListOriginAccessControls	Concede permissão para listar todos os controles de acesso de origem na conta	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListOriginRequestPolicies	Concede permissão para listar todas as políticas de solicitação de origem que foram criadas CloudFront para esta conta	Lista			
ListPublicKeys	Concede permissão para listar todas as chaves públicas que foram adicionadas CloudFront a essa conta	Lista			
ListRateCards [somente permissão]	Concede permissão para listar CloudFront tabelas de preços para a conta	Lista			
ListRealtimeLogConfigs	Concede permissão para obter uma lista de configurações de log em tempo real	Lista			
ListResponseHeadersPolicies	Concede permissão para listar todas as políticas de cabeçalhos de resposta que foram criadas CloudFront para essa conta	Lista			
ListSavingsPlans [somente permissão]	Concede permissão para listar savings plans na conta	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListStreamingDistributions	Concede permissão para listar suas distribuições RMTP	Lista			
ListTagsForResource	Concede permissão para listar tags para um CloudFront recurso	Leitura	anycast-ip-list		
			connection-group		
			distribution		
			distribution-tenant		
			vpcorigin		
ListUsages [somente permissão]	Concede permissão para listar o CloudFront uso	Lista			
ListVpcOrigins	Concede permissão para listar as origens da VPC	Lista			
PublishFunction	Concede permissão para publicar uma CloudFront função	Gravar	function*		
TagResource	Concede permissão para adicionar tags a um CloudFront recurso	Tags	anycast-ip-list		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			connection-group		
			distribution		
			distribution-tenant		
			streaming-distribution		
			vpcorigin		
				aws:RequestTag/${TagKey} aws:TagKeys	
TestFunction	Concede permissão para testar uma CloudFront função	Gravar	function*		
UntagResource	Concede permissão para remover tags de um CloudFront recurso	Tags	anycast-ip-list		
			connection-group		
			distribution		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			distribution-tenant		
			streaming-distribution		
			vpcorigin		
				aws:TagKeys	
UpdateCachePolicy	Concede permissão para atualizar uma política de cache	Gravar	cache-policy*		
UpdateCloudFrontOriginAccessIdentity	Concede permissão para definir a configuração de uma identidade de acesso de CloudFront origem	Gravar	origin-access-identity*		
UpdateConnectionGroup	Concede permissão para atualizar um grupo de conexão	Gravar	connection-group*		
UpdateContinuousDeploymentPolicy	Concede permissão para atualizar a política de implantação contínua	Gravar	continuous-deployment-policy*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateDistribution	Concede permissão para atualizar a configuração de uma distribuição da Web	Gravar	distribution*		
UpdateDistributionTenant	Concede permissão para atualizar um inquilino de distribuição	Gravar	distribution-tenant*		
UpdateDistributionWithStagingConfig	Concede permissão para copiar a configuração de uma distribuição da Web temporária para a distribuição da Web primária correspondente	Gravar	distribution*		
UpdateDomainAssociation	Concede permissão para atualizar uma associação de domínio	Gravar	distribution		
			distribution-tenant		
UpdateFieldLevelEncryptionConfig	Concede permissão para atualizar uma configuração de criptografia em nível de campo	Write			
UpdateFieldLevelEncryptionProfile	Concede permissão para atualizar um perfil de criptografia em nível de campo	Gravar	field-level-encryption-profile*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateFunction	Concede permissão para atualizar uma CloudFront função	Gravar	function*		
UpdateKeyGroup	Concede permissão para atualizar um grupo de chaves	Gravar			
UpdateKeyValueStore	Concede permissão para atualizar um CloudFront KeyValueStore	Gravar	key-value-store*		
UpdateOriginAccessControl	Concede permissão para atualizar um controle de acesso de origem	Gravar	origin-access-control*		
UpdateOriginRequestPolicy	Concede permissão para atualizar uma política de solicitação de origem	Write	origin-request-policy*		
UpdatePublicKey	Concede permissão para atualizar as informações da chave pública	Write			
UpdateRealtimeLogConfig	Concede permissão para atualizar uma configuração de log em tempo real	Gravar	realtime-log-config*		
UpdateResponseHeadersPolicy	Concede permissão para atualizar uma política de cabeçalhos de resposta	Gravar	response-headers-policy*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateSavingsPlan [somente permissão]	Concede permissão para atualizar um savings plan	Gravar			
UpdateStreamingDistribution	Concede permissão para atualizar a configuração de uma distribuição RTMP	Gravar	streaming-distribution*		
UpdateVpcOrigin	Concede permissão para atualizar uma origem de VPC	Gravar	vpcorigin*		
VerifyDnsConfiguration	Concede permissão para verificar a configuração de DNS para um domínio especificado	Leitura	distribution-tenant		

Tipos de recursos definidos pela Amazon CloudFront

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
distribution	`arn:${Partition}:cloudfront::${Account}:distribution/${DistributionId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
streaming-distribution	arn:${Partition}:cloudfront::${Account}:streaming-distribution/${DistributionId}	aws:ResourceTag/${TagKey}
origin-access-identity	arn:${Partition}:cloudfront::${Account}:origin-access-identity/${Id}	
field-level-encryption-config	arn:${Partition}:cloudfront::${Account}:field-level-encryption-config/${Id}	
field-level-encryption-profile	arn:${Partition}:cloudfront::${Account}:field-level-encryption-profile/${Id}	
cache-policy	arn:${Partition}:cloudfront::${Account}:cache-policy/${Id}	
origin-request-policy	arn:${Partition}:cloudfront::${Account}:origin-request-policy/${Id}	
realtime-log-config	arn:${Partition}:cloudfront::${Account}:realtime-log-config/${Name}	
function	arn:${Partition}:cloudfront::${Account}:function/${Name}	
key-value-store	arn:${Partition}:cloudfront::${Account}:key-value-store/${Name}	
response-headers-policy	arn:${Partition}:cloudfront::${Account}:response-headers-policy/${Id}	
origin-access-control	arn:${Partition}:cloudfront::${Account}:origin-access-control/${Id}	

Tipos de recursos	ARN	Chaves de condição
continuous-deployment-policy	arn:${Partition}:cloudfront::${Account}:continuous-deployment-policy/${Id}	
anycast-ip-list	arn:${Partition}:cloudfront::${Account}:anycast-ip-list/${Id}	aws:ResourceTag/${TagKey}
vpcorigin	arn:${Partition}:cloudfront::${Account}:vpcorigin/${Id}	aws:ResourceTag/${TagKey}
distribution-tenant	arn:${Partition}:cloudfront::${Account}:distribution-tenant/${Id}	aws:ResourceTag/${TagKey}
connection-group	arn:${Partition}:cloudfront::${Account}:connection-group/${Id}	aws:ResourceTag/${TagKey}

Chaves de condição para a Amazon CloudFront

A Amazon CloudFront define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String

Chaves de condição	Descrição	Tipo
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para a Amazon CloudFront KeyValueStore

A Amazon CloudFront KeyValueStore (prefixo do serviço:`cloudfront-keyvaluestore`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon CloudFront KeyValueStore
- Tipos de recursos definidos pela Amazon CloudFront KeyValueStore
- Chaves de condição para a Amazon CloudFront KeyValueStore

Ações definidas pela Amazon CloudFront KeyValueStore

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o

nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteKey	Concede permissão para excluir o par chave-valor especificado pela chave	Gravar	key-value-store*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeKeyValueStore	Concede permissão para retornar informações de metadados sobre o Key Value Store	Leitura	key-value-store*		
GetKey	Concede permissão para retornar um par chave-valor	Leitura	key-value-store*		
ListKeys	Concede permissão para retornar uma lista de pares chave-valor	Lista	key-value-store*		
PutKey	Concede permissão para criar um novo par chave-valor ou substituir o valor de uma chave existente	Gravar	key-value-store*		
UpdateKeys	Concede permissão para colocar ou excluir vários pares de valores-chave em uma única all-or-nothing operação	Gravar	key-value-store*		

Tipos de recursos definidos pela Amazon CloudFront KeyValueStore

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
key-value-store	`arn:${Partition}:cloudfront::${Account}:key-value-store/${ResourceId}`	

Chaves de condição para a Amazon CloudFront KeyValueStore

CloudFront KeyValueStore não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS CloudHSM

AWS O CloudHSM (prefixo do serviço`cloudhsm`:) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS CloudHSM
- Tipos de recursos definidos pelo AWS CloudHSM
- Chaves de condição do AWS CloudHSM

Ações definidas pelo AWS CloudHSM

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CopyBackupToRegion	Concede permissão para criar uma cópia de um backup na região especificada	Gravar	backup*		cloudhsm:CopyBackupToRegion cloudhsm:TagResource cloudhsm:UntagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCluster	Concede permissão para criar um novo cluster AWS CloudHSM	Gravar	backup		cloudhsm:TagResource ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:CreateSecurityGroup ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:RevokeSecurityGroupEgress iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateHsm	Concede permissão para criar um novo módulo de segurança de hardware (HSM) no cluster AWS CloudHSM especificado	Gravar	cluster*		ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:RevokeSecurityGroupEgress
DeleteBackup	Concede permissão para excluir o backup especificado do CloudHSM	Gravar	backup*		
DeleteCluster	Concede permissão para excluir o cluster AWS CloudHSM especificado	Gravar	cluster*		ec2:DeleteNetworkInterface ec2:DeleteSecurityGroup
DeleteHsm	Concede permissão para excluir o HSM especificado	Gravar			ec2:DeleteNetworkInterface
DeleteResourcePolicy	Concede permissão para excluir a política anexada aos recursos do CloudHSM	Gravar	backup*		
DescribeBackups	Concede permissão para obter informações sobre backups de clusters do AWS CloudHSM	Leitura			
DescribeClusters	Concede permissão para obter informações sobre clusters do AWS CloudHSM	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetResourcePolicy	Concede permissão para obter informações sobre a política anexada a um recurso do AWS CloudHSM	Leitura	backup*		
InitializeCluster	Concede permissão para reivindicar um cluster AWS CloudHSM	Gravar	cluster*		
ListTags	Concede permissão para obter uma lista de tags para o cluster AWS CloudHSM especificado	Leitura	backup		
			cluster		
ModifyBackupAttributes	Concede permissão para modificar atributos para um backup do AWS CloudHSM	Gravar	backup*		
ModifyCluster	Concede permissão para modificar o cluster do AWS CloudHSM	Gravar	cluster*		ec2:DescribeSubnets
PutResourcePolicy	Concede permissão para anexar uma política a um recurso do AWS CloudHSM	Gravar	backup*		
RestoreBackup	Concede permissão para restaurar o backup especificado do CloudHSM	Gravar	backup*		
TagResource	Concede permissão para adicionar ou substituir uma ou mais tags para o cluster AWS CloudHSM especificado	Tags	backup		
			cluster		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover a tag ou as tags especificadas do cluster AWS CloudHSM especificado	Tags	backup		
			cluster		
				aws:TagKeys	

Tipos de recursos definidos pelo AWS CloudHSM

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
backup	`arn:${Partition}:cloudhsm:${Region}:${Account}:backup/${CloudHsmBackupInstanceName}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
cluster	`arn:${Partition}:cloudhsm:${Region}:${Account}:cluster/${CloudHsmClusterInstanceName}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS CloudHSM

AWS O CloudHSM define as seguintes chaves de condição que podem ser usadas no elemento de uma `Condition` política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para a Amazon CloudSearch

A Amazon CloudSearch (prefixo do serviço:`cloudsearch`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon CloudSearch
- Tipos de recursos definidos pela Amazon CloudSearch
- Chaves de condição para a Amazon CloudSearch

Ações definidas pela Amazon CloudSearch

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de

condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddTags	Anexa tags de recursos a um domínio da Amazon CloudSearch	Tags	domain*		
BuildSuggesters	Indexa as sugestões de pesquisa	Gravar	domain*		
CreateDomain	Cria um novo domínio de pesquisa	Gravar	domain*		
DefineAnalysisScheme	Configura um esquema de análise que pode ser aplicado a um campo de texto ou de matriz de texto para definir opções de processamento de texto específicas ao idioma	Gravar	domain*		
DefineExpression	Configura uma expressão para o domínio de pesquisa	Gravar	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DefineIndexField	Configura um IndexField para o domínio de pesquisa	Gravar	domain*		
DefineSuggester	Configura um sugestor para um domínio	Gravar	domain*		
DeleteAnalysisScheme	Exclui um esquema de análise	Gravar	domain*		
DeleteDomain	Exclui permanentemente um domínio de pesquisa e todos os seus dados	Gravar	domain*		
DeleteExpression	Remove uma expressão do domínio de pesquisa	Gravar	domain*		
DeleteIndexField	Remove um IndexField do domínio de pesquisa	Gravar	domain*		
DeleteSuggester	Exclui um sugestor	Gravar	domain*		
DescribeAnalysisSchemes	Obtém os esquemas de análise configurados para um domínio	Leitura	domain*		
DescribeAvailabilityOptions	Obtém as opções de disponibilidade configuradas para um domínio	Leitura	domain*		
DescribeDomainEndpointOptions	Obtém as opções do endpoint do domínio configuradas para um domínio	Leitura	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeDomains	Obtém informações sobre os domínios de pesquisa pertencentes à conta	Lista	domain*		
DescribeExpressions	Obtém as expressões configuradas para o domínio de pesquisa	Leitura	domain*		
DescribeIndexFields	Obtém informações sobre os campos de índice configurados para o domínio de pesquisa	Leitura	domain*		
DescribeScalingParameters	Obtém os parâmetros de escalabilidade configurados para um domínio	Leitura	domain*		
DescribeServiceAccessPolicies	Obtém informações sobre as políticas de acesso que controlam o acesso aos endpoints de pesquisa e de documentos do domínio	Leitura	domain*		
DescribeSuggesters	Obtém os sugestores configurados para um domínio	Leitura	domain*		
IndexDocuments	Pede para o domínio de pesquisa iniciar a indexação dos seus documentos usando as opções de indexação mais recentes	Gravar	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDomainNames	Lista todos os domínios de pesquisa pertencentes a uma conta	Lista	domain*		
ListTags	Exibe todas as tags de recursos de um CloudSearch domínio da Amazon	Leitura	domain*		
RemoveTags	Remove as etiquetas de recursos especificadas de um domínio do Amazon ES	Tags	domain*		
UpdateAvailabilityOptions	Configura as opções de disponibilidade para um domínio	Gravar	domain*		
UpdateDomainEndpointOptions	Configura as opções do endpoint do domínio para um domínio	Gravar	domain*		
UpdateScalingParameters	Configura os parâmetros de escalabilidade para um domínio	Gravar	domain*		
UpdateServiceAccessPolicies	Configura as regras de acesso que controlam o acesso aos endpoints de pesquisa e de documentos do domínio	Gerenciamento de permissões	domain*		
document [somente permissão]	Permite o acesso às operações do serviço de documentos	Gravar	domain		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
search [somente permissão]	Permite o acesso às operações de pesquisa	Leitura	domain		
suggest [somente permissão]	Permite o acesso às operações de sugestão	Leitura	domain		

Tipos de recursos definidos pela Amazon CloudSearch

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

> **Note**
>
> Para obter informações sobre o uso de CloudSearch recursos da Amazon ARNs em uma política do IAM, consulte Amazon CloudSearch ARNs no Amazon CloudSearch Developer Guide.

Tipos de recursos	ARN	Chaves de condição
domain	`arn:${Partition}:cloudsearch:${Region}:${Account}:domain/${DomainName}`	

Chaves de condição para a Amazon CloudSearch

CloudSearch não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o AWS CloudShell

AWS CloudShell (prefixo do serviço:`cloudshell`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS CloudShell
- Tipos de recursos definidos pelo AWS CloudShell
- Chaves de condição do AWS CloudShell

Ações definidas pelo AWS CloudShell

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos

("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ApproveCommand [somente permissão]	Concede permissão para aprovar um comando enviado por outro serviço AWS	Leitura	Environment*		
CreateEnvironment	Concede permissões para criar um CloudShell ambiente	Gravar		cloudshell:SecurityGroupIds	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
[somente permissão]				cloudshell:SubnetIds cloudshell:VpcIds	
CreateSession [somente permissão]	Concede permissões para se conectar a um CloudShell ambiente a partir do AWS Management Console	Gravar	Environment*		
DeleteEnvironment [somente permissão]	Concede permissão para excluir um CloudShell ambiente	Gravar	Environment*		
DescribeEnvironments [somente permissão]	Concede permissão para retornar descrições de ambientes de usuários existentes	Lista			
GetEnvironmentStatus [somente permissão]	Concede permissão para ler o status de um CloudShell ambiente	Leitura	Environment*		
GetFileDownloadUrls [somente permissão]	Concede permissões para baixar arquivos de um CloudShell ambiente	Gravar	Environment*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetFileUploadUrls [somente permissão]	Concede permissões para carregar arquivos em um CloudShell ambiente	Gravar	Environment*		
PutCredentials [somente permissão]	Concede permissões para encaminhar as credenciais do console para o ambiente	Write	Environment*		
StartEnvironment [somente permissão]	Concede permissão para iniciar um CloudShell ambiente parado	Gravar	Environment*		
StopEnvironment [somente permissão]	Concede permissão para interromper um CloudShell ambiente em execução	Gravar	Environment*		

Tipos de recursos definidos pelo AWS CloudShell

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
Environment	`arn:${Partition}:cloudshell:${Region}:${Account}:environment/${EnvironmentId}`	

Chaves de condição do AWS CloudShell

AWS CloudShell define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
cloudshell:SecurityGroupIds	Filtra o acesso pelos IDs do grupo de segurança. Disponível durante a CreateEnvironment operação	ArrayOfString
cloudshell:SubnetIds	Filtra o acesso por IDs de sub-rede. Disponível durante a CreateEnvironment operação	ArrayOfString
cloudshell:VpcIds	Filtra o acesso por IDs de VPC. Disponível durante a CreateEnvironment operação	ArrayOfString

Ações, recursos e chaves de condição para o AWS CloudTrail

AWS CloudTrail (prefixo do serviço:`cloudtrail`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS CloudTrail
- Tipos de recursos definidos pelo AWS CloudTrail
- Chaves de condição do AWS CloudTrail

Ações definidas pelo AWS CloudTrail

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de

condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddTags	Concede permissão para adicionar uma ou mais tags a uma trilha, armazenamento de dados de eventos, canal ou painel, até um limite de 50	Tags	channel		
			dashboard		
			eventdatastore		
			trail		
				aws:RequestTag/${TagKey} aws:TagKeys	
CancelQuery	Concede permissão para cancelar uma consulta em execução	Gravar	eventdatastore*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateChannel	Concede permissão para criar um canal	Gravar	channel*		cloudtrail:AddTags
			eventdatastore*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDashboard	Concede permissão para criar um painel	Gravar	dashboard*		cloudtrail:AddTags cloudtrail:StartDashboardRefresh cloudtrail:StartQuery
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateEventDataStore	Concede permissão para criar um armazenamento de dados de evento	Gravar	eventdatastore*		cloudtrail:AddTags iam:CreateServiceLinkedRole iam:GetRole kms:Decrypt kms:GenerateDataKey organizations:ListAWSServiceAccessForOrganization
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateServiceLinkedChannel [somente permissão]	Concede permissão para criar um canal vinculado ao serviço que especifica as configurações para entrega de dados de log a um serviço AWS	Gravar	channel*		
CreateTrail	Concede permissão para criar uma trilha que especifica as configurações para a entrega de dados de log para um bucket do Amazon S3	Gravar	trail*		cloudtrail:AddTags iam:CreateServiceLinkedRole iam:GetRole organizations:ListAWSServiceAccessForOrganization
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Concede permissão para excluir um canal	Gravar	channel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteDashboard	Concede permissão para excluir um painel	Gravar	dashboard*		
DeleteEventDataStore	Concede permissão para excluir um armazenamento de dados de evento	Gravar	eventdatastore*		
DeleteResourcePolicy	Concede permissão para excluir uma política de recursos do recurso fornecido	Gravar	channel		
			dashboard		
			eventdatastore		
DeleteServiceLinkedChannel [somente permissão]	Concede permissão para excluir um canal vinculado ao serviço	Gravar	channel*		
DeleteTrail	Concede permissão para excluir uma trilha	Gravar	trail*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeregisterOrganizationDelegatedAdmin	Concede permissão para cancelar o registro de uma conta de membro do AWS Organizations como administrador delegado	Gravar			organizations:DeregisterDelegatedAdministrator organizations:ListAWSServiceAccessForOrganization
DescribeQuery	Concede permissão para listar detalhes da consulta	Leitura	eventdatastore*		
DescribeTrails	Concede permissão para listar as configurações das trilhas associadas à região atual de sua conta	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisableFederation	Concede permissão para desativar a federação de dados do armazenamento de dados de eventos usando o AWS Glue Data Catalog	Gravar	eventdatastore*		glue:DeleteDatabase glue:DeleteTable glue:PassConnection lakeformation:DeregisterResource lakeformation:RegisterResource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
EnableFederation	Concede permissão para habilitar a federação de dados do armazenamento de dados de eventos usando o AWS Glue Data Catalog	Gravar	eventdatastore*		glue:CreateDatabase glue:CreateTable iam:GetRole iam:PassRole lakeformation:DeregisterResource lakeformation:RegisterResource
GenerateQuery	Concede permissão para gerar uma consulta para um armazenamento de dados de eventos especificado usando o gerador de consultas CloudTrail Lake	Gravar	eventdatastore*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GenerateQueryResultsSummary [somente permissão]	Concede permissão para gerar um resumo dos resultados para consultas específicas usando o gerador de linguagem CloudTrail natural	Leitura	eventdatastore*		cloudtrail:GetQueryResults kms:Decrypt kms:GenerateDataKey
GetChannel	Concede permissão para retornar informações sobre um canal específico	Leitura	channel*		
GetDashboard	Concede permissão para listar as configurações do painel	Leitura	dashboard*		
GetEventConfiguration	Concede permissão para listar configurações de eventos que estão configuradas para um armazenamento de dados de eventos	Leitura	eventdatastore*		
GetEventDataStore	Concede permissão para listar as configurações do armazenamento de dados de evento	Leitura	eventdatastore*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetEventDataStoreData	Concede permissão para obter dados de um armazenamento de dados de eventos usando o AWS Glue Data Catalog	Leitura	eventdatastore*		kms:Decrypt kms:GenerateDataKey
GetEventSelectors	Concede permissão para listar as configurações de seletores de eventos configurados para uma trilha	Leitura	trail*		
GetImport	Concede permissão para retornar informações sobre uma importação específica	Leitura			
GetInsightSelectors	Concede permissão para listar seletores do CloudTrail Insights que estão configurados para um armazenamento de dados de trilhas ou eventos	Leitura	eventdatastore		
			trail		
GetQueryResults	Concede permissão para buscar resultados de uma consulta concluída	Leitura	eventdatastore*		kms:Decrypt kms:GenerateDataKey
GetResourcePolicy	Concede permissão para obter a política de recursos anexada ao recurso fornecido	Leitura	channel		
			dashboard		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			eventdatastore		
GetServiceLinkedChannel [somente permissão]	Concede permissão para listar as configurações do canal vinculado ao serviço	Leitura	channel*		
GetTrail	Concede permissão para listar as configurações da trilha	Read	trail*		
GetTrailStatus	Concede permissão para recuperar uma lista de informações em formato JSON sobre a trilha especificada	Leitura	trail*		
ListChannels	Concede permissão para listar os canais na conta atual e seus nomes de origem	Lista			
ListDashboards	Concede permissão para listar painéis associados à região atual da sua conta	Lista			
ListEventDataStores	Concede permissão para listar armazenamentos de dados de evento associados à região atual de sua conta	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListImportFailures	Concede permissão para retornar uma lista de falhas para a importação especificada	Leitura			
ListImports	Concede permissão para retornar informações sobre todas as importações ou sobre um conjunto selecionado de importações por ImportStatus ou Destino	Lista			
ListPublicKeys	Concede permissão para listar as chaves públicas cujas chaves privadas foram usadas para assinar arquivos de resumo de trilha em um intervalo de tempo especificado	Leitura			
ListQueries	Concede permissão para listar consultas associadas a um armazenamento de dados de evento	Lista	eventdatastore*		
ListServiceLinkedChannels [somente permissão]	Concede permissão para listar as configurações dos canais associados à região atual de uma conta específica	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTags	Concede permissão para listar as tags de trilhas, armazenamentos de dados de eventos, canais ou painéis na região atual	Leitura	channel		
			dashboard		
			eventdatastore		
			trail		
ListTrails	Concede permissão para listar as configurações das trilhas associadas à região atual de sua conta	Lista			
LookupEvents	Concede permissão para pesquisar e recuperar dados métricos de eventos de atividades de API capturados por aqueles CloudTrail que criam, atualizam ou excluem recursos em sua conta	Leitura			
PutEventConfiguration	Concede permissão para criar e atualizar configurações de eventos para um armazenamento de dados de eventos	Gravar	eventdatastore*		iam:CreateServiceLinkedRole iam:GetRole
PutEventSelectors	Concede permissão para criar e atualizar seletores de eventos para uma trilha	Gravar	trail*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutInsightSelectors	Concede permissão para criar e atualizar seletores do CloudTrail Insights para um armazenamento de dados de trilhas ou eventos	Gravar	eventdatastore		
			trail		
PutResourcePolicy	Concede permissão para anexar uma política de recursos ao recurso fornecido	Gravar	channel		
			dashboard		
			eventdatastore		
RegisterOrganizationDelegatedAdmin	Concede permissão para registrar uma conta de membro do AWS Organizations como administrador delegado	Gravar			iam:CreateServiceLinkedRole iam:GetRole organizations:ListAWSServiceAccessForOrganization organizations:RegisterDelegatedAdministrator

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RemoveTags	Concede permissão para remover tags de uma trilha, armazenamento de dados de eventos, canal ou painel	Tags	channel		
			dashboard		
			eventdatastore		
			trail		
				aws:TagKeys	
RestoreEventDataStore	Concede permissão para restaurar um armazenamento de dados de evento	Gravar	eventdatastore*		
SearchSampleQueries	Concede permissão para realizar pesquisas semânticas para consultas de amostra CloudTrail do Lake	Leitura			
StartDashboardRefresh	Concede permissão para iniciar uma atualização no painel especificado	Gravar	dashboard*		cloudtrail:StartQuery
StartEventDataStoreIngestion	Concede permissão para iniciar a ingestão de um armazenamento de dados de evento	Gravar	eventdatastore*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartImport	Concede permissão para iniciar a importação de eventos de trilha registrados em log de um bucket de origem do S3 para um armazenamento de dados de eventos de destino	Gravar			
StartLogging	Concede permissão para iniciar a gravação de chamadas de AWS API e a entrega de arquivos de log para uma trilha	Gravar	trail*		
StartQuery	Concede permissão para iniciar uma nova consulta em um armazenamento de dados de evento especificado	Gravar	eventdatastore*		kms:Decrypt kms:GenerateDataKey
StopEventDataStoreIngestion	Concede permissão para interromper a ingestão de um armazenamento de dados de evento	Gravar	eventdatastore*		
StopImport	Concede permissão para interromper uma importação especificada	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopLogging	Concede permissão para interromper a gravação de chamadas de AWS API e a entrega de arquivos de log para uma trilha	Gravar	trail*		
UpdateChannel	Concede permissão para atualizar um canal	Gravar	channel*		
UpdateDashboard	Concede permissão para atualizar um painel	Gravar	dashboard*		cloudtrail:StartDashboardRefresh cloudtrail:StartQuery

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateEventDataStore	Concede permissão para atualizar um armazenamento de dados de evento	Gravar	eventdatastore*		iam:CreateServiceLinkedRole iam:GetRole kms:Decrypt kms:GenerateDataKey organizations:ListAWSServiceAccessForOrganization
UpdateServiceLinkedChannel [somente permissão]	Concede permissão para atualizar as configurações do canal vinculado ao serviço para entrega de dados de log a um serviço AWS	Gravar	channel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateTrail	Concede permissão para atualizar as configurações que especificam a entrega de arquivos de log	Gravar	trail*		iam:CreateServiceLinkedRole iam:GetRole organizations:ListAWSServiceAccessForOrganization

Tipos de recursos definidos pelo AWS CloudTrail

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

> **Note**
>
> Para políticas que controlam o acesso às CloudTrail ações, o elemento Resource é sempre definido como “*”. Para obter informações sobre o uso de recursos ARNs em uma política do IAM, consulte Como AWS CloudTrail funciona com o IAM no Guia AWS CloudTrail do usuário.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS CloudTrail

AWS CloudTrail define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso pelos pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas anexadas ao recurso	String

Chaves de condição	Descrição	Type
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta em uma solicitação	ArrayOfString

Ações, recursos e chaves de condição para AWS CloudTrail dados

AWS CloudTrail Os dados (prefixo do serviço:`cloudtrail-data`) fornecem os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas por AWS CloudTrail Data
- Tipos de recursos definidos por AWS CloudTrail Data
- Chaves de condição para AWS CloudTrail dados

Ações definidas por AWS CloudTrail Data

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutAuditEvents	Concede permissão para ingerir os eventos do seu aplicativo no Lake CloudTrail	Gravar	channel*		

Tipos de recursos definidos por AWS CloudTrail Data

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

> **Note**
>
> Para políticas que controlam o acesso às CloudTrail ações, o elemento Resource é sempre definido como "*". Para obter informações sobre o uso de recursos ARNs em uma política do IAM, consulte Como AWS CloudTrail funciona com o IAM no Guia AWS CloudTrail do usuário.

Tipos de recursos	ARN	Chaves de condição
channel	`arn:${Partition}:cloudtrail:${Region}:${Account}:channel/${ChannelId}`	aws:ResourceTag/${TagKey}

Chaves de condição para AWS CloudTrail dados

AWS CloudTrail Os dados definem as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso pela chave e valor de uma etiqueta em uma solicitação	String
aws:ResourceTag/${TagKey}	Filtra ações com base na presença de pares de chave-valor da etiqueta na solicitação	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta em uma solicitação	ArrayOfString

Ações, recursos e chaves de condição para a Amazon CloudWatch

A Amazon CloudWatch (prefixo do serviço:`cloudwatch`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon CloudWatch
- Tipos de recursos definidos pela Amazon CloudWatch
- Chaves de condição para a Amazon CloudWatch

Ações definidas pela Amazon CloudWatch

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchGetServiceLevelIndicatorReport	Concede permissão para obter em lote um relatório de indicador de nível de serviço	Leitura			
BatchGetServiceLevelObjectiveBudgetReport	Concede permissão para recuperar em lote um relatório de orçamento objetivo de nível de serviço	Leitura	slo*		
CreateServiceLevelObjective	Concede permissão para criar um objetivo de nível de serviço	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAlarms	Concede permissão para excluir um conjunto de alarmes	Write	alarm*		
DeleteAnomalyDetector	Concede permissão para excluir o modelo de detecção de anomalias especificado da sua conta	Gravar			
DeleteDashboards	Concede permissão para excluir todos os CloudWatch painéis que você especificar	Gravar	dashboard*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteInsightRules	Concede permissão para excluir um conjunto de regras de insight	Gravar	insight-rule*		
DeleteMetricStream	Concede permissão para excluir o fluxo CloudWatch métrico que você especificar	Gravar	metric-stream*		
DeleteServiceLevelObjective	Concede permissão para excluir um objetivo de nível de serviço	Gravar	slo*		
DescribeAlarmHistory	Concede permissão para recuperar o histórico do alarme especificado	Read	alarm*		
DescribeAlarms	Concede permissão para descrever todos os alarmes atualmente pertencentes à conta do usuário	Read	alarm*		
DescribeAlarmsForMetric	Concede permissão para descrever todos os alarmes configurados na métrica especificada, atualmente pertencentes à conta do usuário	Read			
DescribeAnomalyDetectors	Concede permissão para listar os modelos de detecção de anomalias criados na sua conta	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeInsightRules	Concede permissão para descrever todas as regras de insight atualmente pertencentes à conta do usuário	Read			
DisableAlarmActions	Concede permissão para desabilitar ações para um conjunto de alarmes	Write	alarm*		
DisableInsightRules	Concede permissão para desabilitar um conjunto de regras de insight	Write	insight-rule*		
EnableAlarmActions	Concede permissão para habilitar ações para um conjunto de alarmes	Write	alarm*		
EnableInsightRules	Concede permissão para habilitar um conjunto de regras de insight	Gravar	insight-rule*		
EnableTopologyDiscovery	Concede permissão para habilitar uma descoberta de CloudWatch topologia	Gravar			
GenerateQuery	Concede permissão para gerar uma string de consulta do Metrics Insights ou do Logs Insights a partir de um prompt em linguagem natural	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GenerateQueryResultsSummary	Concede permissão para gerar um resumo dos resultados da CloudWatch LogInsights consulta em linguagem natural usando IA generativa	Leitura			
GetDashboard	Concede permissão para exibir os detalhes do CloudWatch painel que você especificar	Leitura	dashboard*		
GetInsightRuleReport	Concede permissão para retornar o relatório dos principais colaboradores exclusivos ao longo de um intervalo para determinada regra de insight	Leitura	insight-rule*		
GetMetricData	Concede permissão para recuperar quantidades em lote de dados CloudWatch métricos e realizar cálculos métricos nos dados recuperados	Leitura			
GetMetricStatistics	Concede permissão para recuperar estatísticas para a métrica especificada	Leitura			
GetMetricStream	Concede permissão para retornar os detalhes de um fluxo CloudWatch métrico	Leitura	metric-stream*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetMetricWidgetImage	Concede permissão para recuperar snapshots de widgets de métrica	Leitura			
GetService	Concede permissão para recuperar informações sobre um serviço	Leitura	service*		
GetServiceData [somente permissão]	Concede permissão para recuperar dados de serviço	Leitura	service*		
GetServiceLevelObjective	Concede permissão para recuperar informações sobre um objetivo de nível de serviço	Leitura	slo*		
GetTopologyDiscoveryStatus [somente permissão]	Concede permissão para recuperar um status de descoberta de CloudWatch topologia	Leitura			
GetTopologyMap	Concede permissão para recuperar um mapa de CloudWatch topologia	Leitura			
Link [somente permissão]	Concede permissão para compartilhar CloudWatch recursos com uma conta de monitoramento	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDashboards	Concede permissão para retornar uma lista de todos os CloudWatch painéis em sua conta	Lista			
ListEntitiesForMetric [somente permissão]	Concede permissão para recuperar todas as entidades que estão emitindo uma determinada métrica	Lista			
ListManagedInsightRules	Concede permissão para listar as regras gerenciadas do Insight disponíveis para um determinado ARN de recurso	Leitura		aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:requestManagedResourceARNs	
ListMetricStreams	Concede permissão para retornar uma lista de todos os fluxos de CloudWatch métricas em sua conta	Lista			
ListMetrics	Concede permissão para recuperar uma lista de métricas válidas armazenadas para o proprietário Conta da AWS	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListServiceLevelObjectives	Concede permissão para listar objetivos de nível de serviço	Lista			
ListServices	Concede permissão para listar serviços	Lista			
ListTagsForResource	Concede permissão para listar tags para um CloudWatch recurso da Amazon	Lista	alarm		
			insight-rule		
			slo		
	CENÁRIO: CloudWatch-Alarm		alarm*		
	CENÁRIO: CloudWatch-InsightRule		insight-rule*		
	CENÁRIO: CloudWatch-ServiceLevelObjective		slo*		
PutAnomalyDetector	Concede permissão para criar ou atualizar um modelo de detecção de anomalias para uma métrica CloudWatch	Gravar			
PutCompositeAlarm	Concede permissão para criar ou atualizar um alarme composto	Gravar	alarm*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:AlarmActions	
PutDashboard	Concede permissão para criar um CloudWatch painel ou atualizar um painel existente, se ele já existir	Gravar	dashboard*		
PutInsightRule	Concede permissão para criar uma nova regra de insight ou substituir uma regra de insight existente	Gravar	insight-rule*		
				aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:requestInsightRuleLogGroups	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutManagedInsightRules	Concede permissão para criar regras gerenciadas do Insight	Gravar		aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:requestManagedResourceARNs	
PutMetricAlarm	Concede permissão para criar ou atualizar um alarme e o associa à métrica especificada da Amazon CloudWatch	Gravar	alarm*		
				aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:AlarmActions	
PutMetricData	Concede permissão para publicar pontos de dados métricos na Amazon CloudWatch	Gravar		cloudwatch:namespace	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutMetricStream	Concede permissão para criar um fluxo CloudWatch métrico ou atualizar um fluxo métrico existente, se ele já existir	Gravar	metric-stream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
SetAlarmState	Concede permissão para definir temporariamente o estado de um alarme para fins de teste	Gravar	alarm*		
StartMetricStreams	Concede permissão para iniciar todos os fluxos CloudWatch métricos que você especificar	Gravar	metric-stream*		
StopMetricStreams	Concede permissão para interromper todos os fluxos CloudWatch métricos que você especificar	Gravar	metric-stream*		
TagResource	Concede permissão para adicionar tags a um CloudWatch recurso da Amazon	Tags	alarm		
			insight-rule		
			slo		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
	CENÁRIO: CloudWatch-Alarm		alarm*		
	CENÁRIO: CloudWatch-InsightRule		insight-rule*		
	CENÁRIO: CloudWatch-ServiceLevelObjective		slo*		
UntagResource	Concede permissão para remover uma tag de um CloudWatch recurso da Amazon	Tags	alarm		
			insight-rule		
			slo		
				aws:TagKeys	
	CENÁRIO: CloudWatch-Alarm		alarm*		
	CENÁRIO: CloudWatch-InsightRule		insight-rule*		
	CENÁRIO: CloudWatch-ServiceLevelObjective		slo*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateServiceLevelObjective	Concede permissão para atualizar um objetivo de nível de serviço	Gravar	slo*		

Tipos de recursos definidos pela Amazon CloudWatch

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
service	`arn:${Partition}:cloudwatch:${Region}:${Account}:service/${ServiceName}-${UniqueAttributesHex}`	aws:ResourceTag/${TagKey}

Chaves de condição para a Amazon CloudWatch

A Amazon CloudWatch define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base no conjunto de valores permitidos para cada uma das etiquetas	String
aws:ResourceTag/${TagKey}	Filtra ações com base no etiqueta-value associado ao recurso	String
aws:TagKeys	Filtra ações com base na presença de etiquetas obrigatórias na solicitação	ArrayOfString
cloudwatch:AlarmActions	Filtra ações com base em ações de alarme definidas	ArrayOfString
cloudwatch:namespace	Filtra ações com base na presença de valores de namespace opcionais	String
cloudwatch:request	Filtra ações com base nos grupos de log especificados em uma regra de insight	ArrayOfString

Chaves de condição	Descrição	Type
InsightRuleLogGroups		
cloudwatch:requestManagedResourceARNs	Filtra o acesso pelo recurso ARNs especificado em uma regra gerenciada do Insight	ArrayOfARN

Ações, recursos e chaves de condição para o Amazon CloudWatch Application Insights

O Amazon CloudWatch Application Insights (prefixo do serviço:`applicationinsights`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon CloudWatch Application Insights
- Tipos de recursos definidos pelo Amazon CloudWatch Application Insights
- Chaves de condição para o Amazon CloudWatch Application Insights

Ações definidas pelo Amazon CloudWatch Application Insights

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddWorkload	Concede permissão para adicionar uma workload	Gravar			
CreateApplication	Concede permissão para criar uma aplicação a partir de um grupo de recursos	Write			
CreateComponent	Concede permissão para criar um componente a partir de um grupo de recursos	Write			
CreateLogPattern	Concede permissão para criar log de um padrão	Write			
DeleteApplication	Concede permissão para excluir um aplicativo	Write			
DeleteComponent	Concede permissão para excluir um componente	Write			
DeleteLogPattern	Concede permissão para excluir um padrão de log	Write			
DescribeApplication	Concede permissão para descrever um ativo	Read			
DescribeComponent	Concede permissão para descrever um componente	Read			
DescribeComponentConfiguration	Concede permissão para descrever a configuração de um componente	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeComponentConfigurationRecommendation	Concede permissão para descrever a configuração recomendada do componente da aplicação	Read			
DescribeLogPattern	Concede permissão para descrever um padrão de log	Read			
DescribeObservation	Concede permissão para descrever uma observação	Read			
DescribeProblem	Concede permissão para descrever um problema	Read			
DescribeProblemObservations	Concede permissão para descrever a observação em um problema	Leitura			
DescribeWorkload	Concede permissão para descrever uma workload	Leitura			
Link [somente permissão]	Concede permissão para compartilhar recursos do Application Insights com uma conta de monitoramento	Gravar			
ListApplications	Concede permissão para listar todos as aplicações	List			
ListComponents	Concede permissão para listar os componentes de uma aplicação	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListConfigurationHistory	Concede permissão para listar o histórico de configuração	List			
ListLogPatternSets	Concede permissão para listar conjuntos de padrões de log para uma aplicação	List			
ListLogPatterns	Concede permissão para listar padrões de log	List			
ListProblems	Concede permissão para listar os problemas em uma aplicação	List			
ListTagsForResource	Concede permissão para listar etiquetas para o recurso	Leitura			
ListWorkloads	Concede permissão para listar cargas de trabalho	Lista			
RemoveWorkload	Concede permissão para remover uma workload	Gravar			
TagResource	Concede permissão para marcar um recurso	Marcação		aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso	Marcação		aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateApplication	Concede permissão para atualizar uma aplicação	Write			
UpdateComponent	Concede permissão para atualizar um componente	Write			
UpdateComponentConfiguration	Concede permissão para atualizar a configuração de um componente	Write			
UpdateLogPattern	Concede permissão para atualizar um padrão de log	Gravar			
UpdateProblem	Concede permissão para atualizar um problema	Gravar			
UpdateWorkload	Concede permissão para atualizar uma workload	Gravar			

Tipos de recursos definidos pelo Amazon CloudWatch Application Insights

O Amazon CloudWatch Application Insights não suporta a especificação de um ARN de recurso `Resource` no elemento de uma declaração de política do IAM. Para permitir o acesso ao Amazon CloudWatch Application Insights, especifique `"Resource": "*"` em sua política.

Chaves de condição para o Amazon CloudWatch Application Insights

O Amazon CloudWatch Application Insights define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por um par de chave valor da etiqueta que é permitido na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso por um par de chave e valor da etiqueta de um recurso.	Segmento
aws:TagKeys	Filtra o acesso por uma lista de chaves da etiqueta que são permitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para Amazon CloudWatch Application Signals

O Amazon CloudWatch Application Signals (prefixo do serviço:`application-signals`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon CloudWatch Application Signals
- Tipos de recursos definidos pelo Amazon CloudWatch Application Signals
- Chaves de condição para Amazon CloudWatch Application Signals

Ações definidas pelo Amazon CloudWatch Application Signals

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando

usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchGetServiceLevelObjectiveBudgetReport	Concede permissão para recuperar em lote um relatório de orçamento objetivo de nível de serviço	Leitura	slo*		
BatchUpdateExclusionWindows	Concede permissão para adicionar ou remover janelas de exclusão da Amazon CloudWatch SLOs	Gravar	slo*		
CreateServiceLevelObjective	Concede permissão para criar um objetivo de nível de serviço	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteServiceLevelObjective	Concede permissão para excluir um objetivo de nível de serviço	Gravar	slo*		
GetService	Concede permissão para recuperar informações sobre um serviço	Leitura			
GetServiceLevelObjective	Concede permissão para recuperar informações sobre um objetivo de nível de serviço	Leitura	slo*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
Link [somente permissão]	Concede permissão para compartilhar recursos do Application Signals com uma conta de monitoramento	Gravar			
ListObservedEntities	Concede permissão para listar entidades associadas a outras entidades	Lista			
ListServiceDependencies	Concede permissão para listar dependências de serviços	Leitura			
ListServiceDependents	Concede permissão para listar dependentes de serviços	Leitura			
ListServiceLevelObjectiveExclusionWindows	Concede permissão para listar janelas de exclusão para um Amazon CloudWatch SLO	Lista	slo*		
ListServiceLevelObjectives	Concede permissão para listar objetivos de nível de serviço	Lista			
ListServiceOperations	Concede permissão para listar operações de serviços	Leitura			
ListServices	Concede permissão para listar serviços	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar tags para um Amazon CloudWatch SLO	Leitura	slo*		
StartDiscovery	Concede permissão para permitir a CloudWatch descoberta	Gravar			
TagResource	Concede permissão para adicionar tags a um Amazon CloudWatch SLO	Tags	slo*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover a tag de um Amazon CloudWatch SLO	Tags	slo*		
				aws:TagKeys	
UpdateServiceLevelObjective	Concede permissão para atualizar um objetivo de nível de serviço	Gravar	slo*		

Tipos de recursos definidos pelo Amazon CloudWatch Application Signals

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves

são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
slo	`arn:${Partition}:application-signals:${Region}:${Account}:slo/${SloName}`	aws:ResourceTag/${TagKey}

Chaves de condição para Amazon CloudWatch Application Signals

O Amazon CloudWatch Application Signals define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelo conjunto de valores permitido para cada uma das etiquetas	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelo valor-etiqueta associado ao recurso	String
aws:TagKeys	Filtra o acesso pela presença de etiquetas obrigatórias na solicitação	ArrayOfString

Ações, recursos e chaves de condição para a Amazon CloudWatch Evidently

O Amazon CloudWatch Evidently (prefixo do serviço:`evidently`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon CloudWatch Evidently
- Tipos de recursos definidos pela Amazon CloudWatch Evidently
- Chaves de condição para Amazon CloudWatch Evidently

Ações definidas pela Amazon CloudWatch Evidently

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar

a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchEvaluateFeature	Concede permissão para enviar uma solicitação de avaliação de recurso em lote	Gravar	Feature*		
CreateExperiment	Concede permissão para criar um experimento	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateFeature	Concede permissão para criar um recurso	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLaunch	Concede permissão para criar um lançamento	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProject	Concede permissão para criar um projeto	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole iam:GetRole
CreateSegment	Concede permissão para criar um segmento	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteExperiment	Concede permissão para excluir um experimento	Gravar	Experiment*		
DeleteFeature	Concede permissão para excluir um recurso	Gravar	Feature*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteLaunch	Concede permissão para excluir um lançamento	Gravar	Launch*		
DeleteProject	Concede permissão para excluir um projeto	Gravar	Project*		
DeleteSegment	Concede permissão para excluir um segmento	Gravar	Segment*		
EvaluateFeature	Concede permissão para enviar uma solicitação de avaliação de recurso	Gravar	Feature*		
GetExperiment	Concede permissão para obter detalhes do experimento	Leitura	Experiment*		
GetExperimentResults	Concede permissão para obter resultado do experimento	Leitura	Experiment*		
GetFeature	Concede permissão para obter detalhes do recurso	Leitura	Feature*		
GetLaunch	Concede permissão para obter detalhes de lançamento	Leitura	Launch*		
GetProject	Concede permissão para obter detalhes do projeto	Leitura	Project*		
GetSegment	Concede permissão para obter detalhes do segmento	Leitura	Segment*		
ListExperiments	Concede permissão para listar experimentos	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListFeatures	Concede permissão para listar recursos	Leitura			
ListLaunches	Concede permissão para listar lançamentos	Leitura			
ListProjects	Concede permissão para listar projetos	Leitura			
ListSegmentReferences	Concede permissão para listar recursos que referenciam um segmento	Leitura			
ListSegments	Concede permissão para listar segmentos	Leitura			
ListTagsForResource	Concede permissão para listar as etiquetas para recursos	Leitura			
PutProjectEvents	Concede permissão para enviar eventos de performance	Gravar	Project*		
StartExperiment	Concede permissão para iniciar um experimento	Gravar	Experiment*		
StartLaunch	Concede permissão para iniciar um lançamento	Gravar	Launch*		
StopExperiment	Concede permissão para interromper um experimento	Gravar	Experiment*		
StopLaunch	Concede permissão para interromper um lançamento	Gravar	Launch*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para marcar recursos	Tags	Experiment		
			Feature		
			Launch		
			Project		
			Segment		
				aws:RequestTag/${TagKey} aws:TagKeys	
TestSegmentPattern	Concede permissão para testar um padrão de segmento	Leitura			
UntagResource	Concede permissão para desmarcar recursos	Tags	Experiment		
			Feature		
			Launch		
			Project		
			Segment		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateExperiment	Concede permissão para atualizar experimento	Gravar	Experiment*		
UpdateFeature	Concede permissão para atualizar recurso	Gravar	Feature*		
UpdateLaunch	Concede permissão para atualizar um lançamento	Gravar	Launch*		
UpdateProject	Concede permissão para atualizar projeto	Gravar	Project*		iam:CreateServiceLinkedRole iam:GetRole
UpdateProjectDataDelivery	Concede permissão para atualizar uma entrega de dados do projeto	Gravar	Project*		

Tipos de recursos definidos pela Amazon CloudWatch Evidently

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
Project	`arn:${Partition}:evidently:${Region}:${Account}:project/${ProjectName}`	aws:ResourceTag/${TagKey}
Feature	`arn:${Partition}:evidently:${Region}:${Account}:project/${ProjectName}/feature/${FeatureName}`	aws:ResourceTag/${TagKey}
Experiment	`arn:${Partition}:evidently:${Region}:${Account}:project/${ProjectName}/experiment/${ExperimentName}`	aws:ResourceTag/${TagKey}
Launch	`arn:${Partition}:evidently:${Region}:${Account}:project/${ProjectName}/launch/${LaunchName}`	aws:ResourceTag/${TagKey}
Segment	`arn:${Partition}:evidently:${Region}:${Account}:segment/${SegmentName}`	aws:ResourceTag/${TagKey}

Chaves de condição para Amazon CloudWatch Evidently

CloudWatch Evidentemente, a Amazon define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que fazem a solicitação em nome do primário do IAM	String

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso que fazem a solicitação em nome do primário do IAM	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação em nome do primário do IAM	ArrayOfString

Ações, recursos e chaves de condição para o Amazon CloudWatch Internet Monitor

O Amazon CloudWatch Internet Monitor (prefixo do serviço:`internetmonitor`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon CloudWatch Internet Monitor
- Tipos de recursos definidos pelo Amazon CloudWatch Internet Monitor
- Chaves de condição para o Amazon CloudWatch Internet Monitor

Ações definidas pelo Amazon CloudWatch Internet Monitor

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateMonitor	Concede permissão para criar um monitor	Gravar	Monitor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteMonitor	Concede permissão para excluir um monitor	Gravar	Monitor*		
GetHealthEvent	Concede permissão para obter informações sobre uma evento de integridade para um monitor especificado	Leitura	Monitor*		
GetInternetEvent	Concede permissão para obter informações sobre um evento da Internet especificado	Leitura	InternetEvent*		
GetMonitor	Concede permissão para obter informações sobre um monitor	Leitura	Monitor*		
GetQueryResults	Concede permissão para obter resultados para uma consulta de dados para um monitor	Leitura	Monitor*		
GetQueryStatus	Concede permissão para obter status para uma	Leitura	Monitor*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	consulta de dados para um monitor				
Link [somente permissão]	Concede permissão para compartilhar recursos do monitor de Internet com uma conta de monitoramento	Gravar			
ListHealthEvents	Concede permissão para listar todos os eventos de integridade de um monitor	Lista	Monitor*		
ListInternetEvents	Concede permissão para listar todos os eventos da Internet	Lista			
ListMonitors	Concede permissão para listar todos os monitores em uma conta e seus status	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	Monitor*		
StartQuery	Concede permissão para iniciar uma consulta de dados para um monitor	Leitura	Monitor*		
StopQuery	Concede permissão para interromper uma consulta de dados para um monitor	Leitura	Monitor*		
TagResource	Concede permissão para adicionar tags da a um recurso	Marcação	Monitor*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover etiquetas de um recurso	Tags	Monitor*		
				aws:TagKeys	
UpdateMonitor	Concede permissão para atualizar um monitor	Gravar	Monitor*		

Tipos de recursos definidos pelo Amazon CloudWatch Internet Monitor

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
HealthEvent	`arn:${Partition}:internetmonitor:${Region}:${Account}:monitor/${MonitorName}/health-event/${EventId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
Monitor	`arn:${Partition}:internetmonitor:${Region}:${Account}:monitor/${MonitorName}`	aws:ResourceTag/${TagKey}
InternetEvent	`arn:${Partition}:internetmonitor::${Account}:internet-event/${InternetEventId}`	

Chaves de condição para o Amazon CloudWatch Internet Monitor

O Amazon CloudWatch Internet Monitor define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para Amazon CloudWatch Logs

O Amazon CloudWatch Logs (prefixo do serviço:`logs`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon CloudWatch Logs
- Tipos de recursos definidos pelo Amazon CloudWatch Logs
- Chaves de condição para Amazon CloudWatch Logs

Ações definidas pelo Amazon CloudWatch Logs

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateKmsKey	Concede permissão para associar a AWS chave mestra de cliente (CMK) do Serviço de Gerenciamento de Chaves (AWS KMS) especificada ao grupo de registros especificado	Gravar	log-group*		
CancelExportTask	Concede permissão para cancelar uma tarefa de exportação se ela estiver no estado PENDING (PENDENTE) ou RUNNING (EM EXECUÇÃO)	Gravar			
CreateDelivery	Concede permissão para criar uma entrega conectando uma	Gravar	delivery*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	fonte de entrega a um destino de entrega		delivery-destination*		
			delivery-source*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateExportTask	Concede permissão para criar um ExportTask que permite exportar com eficiência dados de um grupo de registros para seu bucket do Amazon S3	Gravar	log-group*		
CreateLogAnomalyDetector	Concede permissão para criar um detector de anomalias de logs	Gravar	log-group*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateLogDelivery [somente permissão]	Concede permissão para criar a entrega de logs	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateLogGroup	Concede permissão para criar um novo grupo de logs com o nome especificado	Gravar	log-group*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateLogStream	Concede permissões para criar um novo fluxo de logs com o nome especificado	Gravar	log-stream*		
DeleteAccountPolicy	Concede permissão para excluir uma política de conta	Gravar			
DeleteDataProtectionPolicy	Concede permissão para excluir uma política de proteção de dados anexada a um grupo de logs	Gravar	log-group*		
DeleteDelivery	Concede permissão para excluir uma entrega	Gravar	delivery*		
DeleteDeliveryDestination	Concede permissão para excluir um destino de entrega depois que todas as entregas associadas forem excluídas	Gravar	delivery-destination*		
DeleteDeliveryDestinationPolicy	Concede permissão para excluir uma política de destino de entrega associada a um destino de entrega	Gravar	delivery-destination*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteDeliverySource	Concede permissão para excluir uma origem de entrega depois que todas as entregas associadas forem excluídas	Gravar	delivery-destination*		
DeleteDestination	Concede permissão para excluir o destino com o nome especificado	Gravar	destination*		
DeleteIndexPolicy	Concede permissão para excluir uma política de índice anexada a um grupo de registros	Gravar			
DeleteIntegration	Concede permissão para excluir a integração	Gravar			
DeleteLogAnomalyDetector	Concede permissão para excluir um detector de anomalias de logs	Gravar	anomaly-detector*		
DeleteLogDelivery [somente permissão]	Concede permissão para excluir as informações de entrega de log para a entrega de log especificada	Gravar			
DeleteLogGroup	Concede permissão para excluir o grupo de logs com o nome especificado	Gravar	log-group*		
DeleteLogStream	Concede permissão para excluir um fluxo de logs	Gravar	log-stream*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteMetricFilter	Concede permissão para excluir um filtro de métricas associado ao grupo de logs especificado	Gravar	log-group*		
DeleteQueryDefinition	Concede permissão para excluir uma definição de consulta salva do CloudWatch Logs Insights	Gravar			
DeleteResourcePolicy	Concede permissão para excluir uma política de recursos desta conta	Gerenciamento de permissões			
DeleteRetentionPolicy	Concede permissão para excluir a política de retenção do grupo de logs especificado	Gravar	log-group*		
DeleteSubscriptionFilter	Concede permissão para excluir um filtro de assinaturas associado ao grupo de logs especificado	Gravar	log-group*		
DeleteTransformer	Concede permissão para excluir um transformador associado ao grupo de registros especificado	Gravar	log-group*		
DescribeAccountPolicies	Concede permissão para recuperar as políticas da conta	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeConfigurationTemplates	Concede permissão para recuperar uma lista de modelos de configuração dos tipos de log disponíveis	Lista			
DescribeDeliveries	Concede permissão para recuperar uma lista de entregas em uma conta	Lista			
DescribeDeliveryDestinations	Concede permissão para recuperar uma lista de destinos de entregas em uma conta	Lista			
DescribeDeliverySources	Concede permissão para recuperar uma lista de origens de entregas em uma conta	Lista			
DescribeDestinations	Concede permissão para retornar todos os destinos associados Conta da AWS à solicitação	Lista			
DescribeExportTasks	Concede permissão para retornar todas as tarefas de exportação Conta da AWS associadas à solicitação	Lista			
DescribeFieldIndexes	Concede permissão para retornar todos os atributos de indexação que estão anexados aos grupos de registros	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeIndexPolicies	Concede permissão para retornar todas as políticas de índice que estão anexadas aos grupos de registros	Lista			
DescribeLogGroups	Concede permissão para retornar todos os grupos de registros Conta da AWS associados à solicitação	Lista			
DescribeLogStreams	Concede permissão para retornar todos os fluxos de logs associados ao grupo de logs especificado	Lista	log-group *		
DescribeMetricFilters	Concede permissão para retornar todos os filtros de métricas associados ao grupo de logs especificado	Lista	log-group *		
DescribeQueries	Concede permissão para retornar uma lista de consultas do CloudWatch Logs Insights que estão agendadas, em execução ou que foram executadas recentemente nesta conta	Lista			
DescribeQueryDefinitions	Concede permissão para retornar uma lista paginada de suas definições de consulta salvas do CloudWatch Logs Insights	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeResourcePolicies	Concede permissão para retornar todas as políticas de recursos nesta conta	Lista			
DescribeSubscriptionFilters	Concede permissão para retornar todos os filtros de assinaturas associados ao grupo de logs especificado	Lista	log-group*		
DisassociateKmsKey	Concede permissão para desassociar a AWS chave mestra de cliente (CMK) do Key Management Service (AWS KMS) associada do grupo de registros especificado	Gravar	log-group*		
FilterLogEvents	Concede permissão para recuperar os eventos de logs, opcionalmente filtrados por um padrão de filtro do grupo de logs especificado	Leitura	log-group*		
GetDataProtectionPolicy	Concede permissão para recuperar uma política de proteção de dados anexada a um grupo de logs	Leitura	log-group*		
GetDelivery	Concede permissão para recuperar uma única entrega	Leitura	delivery*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetDeliveryDestination	Concede permissão para recuperar um único destino de entrega	Leitura	delivery-destination*		
GetDeliveryDestinationPolicy	Concede permissão para recuperar uma política de destino de entrega anexada a um destino de entrega	Leitura	delivery-destination*		
GetDeliverySource	Concede permissão para recuperar a origem de uma única entrega	Leitura	delivery-source*		
GetIntegration	Concede permissão para recuperar uma única integração	Leitura			
GetLogAnomalyDetector	Concede permissão para obter um detector de anomalias de logs	Leitura	anomaly-detector*		
GetLogDelivery [somente permissão]	Concede permissão para obter as informações de entrega de log para a entrega de log especificada	Leitura			
GetLogEvents	Concede permissão para recuperar os eventos de logs do fluxo de logs especificado	Leitura	log-stream*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetLogGroupFields	Concede permissão para retornar uma lista dos campos que estão incluídos em eventos de logs no grupo de logs especificado, junto com a porcentagem de eventos de logs que contêm cada campo	Leitura	log-group *		
GetLogRecord	Concede permissão para recuperar todos os campos e valores de um único evento de logs	Leitura	log-group *		
GetQueryResults	Concede permissão para retornar os resultados da consulta especificada	Leitura	log-group *		
GetTransformer	Concede permissão para retornar o transformador associado ao grupo de log especificado	Leitura	log-group *		
Link [somente permissão]	Concede permissão para compartilhar CloudWatch recursos com uma conta de monitoramento	Gravar			
ListAnomalies	Concede permissão para listar todas as anomalias detectadas ao Conta da AWS fazer a solicitação	Lista	anomaly-detector		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListEntitiesForLogGroup [somente permissão]	Concede permissão para recuperar todas as entidades associadas ao grupo de registros	Lista			
ListIntegrations	Concede permissão para listar todas as integrações associadas Conta da AWS à solicitação	Lista			
ListLogAnomalyDetectors	Concede permissão para retornar todos os detectores de anomalias associados à Conta da AWS solicitação	Lista	anomaly-detector		
ListLogDeliveries [somente permissão]	Concede permissão para listar todas as entregas de registros da fonte de and/or registro da conta especificada	Lista			
ListLogGroups	Concede permissão para retornar todos os grupos de registros Conta da AWS associados à solicitação	Lista			
ListLogGroupsForEntity [somente permissão]	Concede permissão para recuperar todos os grupos de registros associados à entidade	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListLogGroupsForQuery	Concede permissão para retornar todos os grupos de registros associados à consulta especificada	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas para o recurso especificado	Lista	anomaly-detector		
			delivery		
			delivery-destination		
			delivery-source		
			destination		
			log-group		
ListTagsLogGroup	Concede permissão para listar as etiquetas para o grupo de logs especificado	Lista	log-group *		
PutAccountPolicy	Concede permissão para anexar uma política de conta	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutDataProtectionPolicy	Concede permissão para anexar uma política de proteção de dados para detectar e editar informações confidenciais de eventos de logs	Gravar	log-group*		
PutDeliveryDestination	Concede permissão a create/update um destino de entrega	Gravar	delivery-destination*		
				aws:TagKeys aws:RequestTag/${TagKey} logs:DeliveryDestinationResourceArn	
PutDeliveryDestinationPolicy	Concede permissão para anexar uma política de destino de entrega a um destino de entrega	Gravar	delivery-destination*		
PutDeliverySource	Concede permissão a create/update uma fonte de entrega	Gravar	delivery-source*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey} logs:LogGeneratingResourceArns	
PutDestination	Concede permissão para criar ou atualizar um destino	Gravar	destination*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey}	
PutDestinationPolicy	Concede permissão para criar ou atualizar uma política de acesso associada a um destino existente	Gravar	destination*		
PutIndexPolicy	Concede permissão para anexar uma política de índice no nível do grupo de registros para otimizar a pesquisa e a consulta	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutIntegration	Concede permissão para criar integração entre o cloudwatch logs e o opensearch	Gravar			
PutLogEvents	Concede permissão para fazer upload de lotes de eventos de logs no fluxo de logs especificado	Gravar	log-stream*		
PutMetricFilter	Concede permissão para criar ou atualizar um filtro de métricas e associá-lo ao grupo de logs especificado	Gravar	log-group*		
PutQueryDefinition	Concede permissão para criar ou atualizar uma definição de consulta	Gravar			
PutResourcePolicy	Concede permissão para criar ou atualizar uma política de recursos, permitindo que outros AWS serviços coloquem eventos de log nessa conta	Gerenciamento de permissões			
PutRetentionPolicy	Concede permissão para definir a retenção do grupo de logs especificado	Gravar	log-group*		
PutSubscriptionFilter	Concede permissão para criar ou atualizar um filtro de assinaturas e associá-o ao grupo de logs especificado	Gravar	log-group*		iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			destination		
PutTransformer	Concede permissão para criar ou atualizar um transformador e o associa ao grupo de registros especificado	Gravar	log-group *		
StartLiveTail	Concede permissão para iniciar uma sessão do Live Tail no CloudWatch Logs	Leitura	log-group *		
StartQuery	Concede permissão para agendar uma consulta de um grupo de CloudWatch registros usando o Logs Insights	Leitura	log-group *		
StopLiveTail [somente permissão]	Concede permissão para interromper uma sessão Live Tail em andamento	Leitura			
StopQuery	Concede permissão para interromper uma consulta do CloudWatch Logs Insights que está em andamento	Leitura			
TagLogGroup	Concede permissão para adicionar ou atualizar as etiquetas especificadas para o grupo de logs especificado	Tags	log-group *		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
TagResource	Concede permissão para adicionar ou atualizar as etiquetas especificadas no recurso especificado	Tags	anomaly-detector		
			delivery		
			delivery-destination		
			delivery-source		
			destination		
			log-group		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TestMetricFilter	Concede permissão para testar o padrão de filtro de um filtro de métricas em relação a um exemplo de mensagens de eventos de log	Leitura			
TestTransformer	Concede permissão para testar o transformador em relação a uma amostra de mensagens de eventos de log	Leitura			
Unmask [somente permissão]	Concede permissão para buscar eventos de logs não mascarados que foram editados com uma política de proteção de dados	Leitura	log-group *		
UntagLogGroup	Concede permissão para remover as etiquetas especificadas do grupo de logs especificado	Tags	log-group *		
				aws:TagKeys	
UntagResource	Concede permissão para remover as etiquetas especificadas do recurso especificado	Tags	anomaly-detector		
			delivery		
			delivery-destination		
			delivery-source		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			destination		
			log-group		
				aws:TagKeys	
UpdateAnomaly	Concede permissão para atualizar uma anomalia relatada por um detector de anomalias de logs	Gravar	anomaly-detector*		
UpdateDeliveryConfiguration	Concede permissão para atualizar a configuração relacionada a uma entrega	Gravar	delivery*		
			delivery-destination*		
			delivery-source*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateLogAnomalyDetector	Concede permissão para atualizar um detector de anomalias de logs	Gravar	anomaly-detector*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateLogDelivery [somente permissão]	Concede permissão para atualizar as informações de entrega de log para a entrega de log especificada	Gravar			

Tipos de recursos definidos pelo Amazon CloudWatch Logs

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição para Amazon CloudWatch Logs

O Amazon CloudWatch Logs define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Chaves de condição	Descrição	Tipo
logs:DeliveryDestinationResourceArn	Filtra o acesso pelo ARN de destino do log que é transmitido na solicitação	ARN
logs:LogGenerating ResourceArns	Filtra o acesso pelo recurso gerador de log ARNs passado na solicitação	ArrayOfARN

Ações, recursos e chaves de condição para o Amazon CloudWatch Network Synthetic Monitor

O Amazon CloudWatch Network Synthetic Monitor (prefixo do serviço:`networkmonitor`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon CloudWatch Network Synthetic Monitor
- Tipos de recursos definidos pelo Amazon CloudWatch Network Synthetic Monitor
- Chaves de condição para o Amazon CloudWatch Network Synthetic Monitor

Ações definidas pelo Amazon CloudWatch Network Synthetic Monitor

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou

ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateMonitor	Concede permissão para criar um monitor	Gravar	monitor*		
CreateProbe	Concede permissão para criar um teste	Gravar			
DeleteMonitor	Concede permissão para excluir um monitor	Gravar	monitor*		
DeleteProbe	Concede permissão para excluir um teste	Gravar	probe*		
GetMonitor	Concede permissão para obter informações sobre um monitor	Leitura	monitor*		
GetProbe	Concede permissão para obter informações sobre um teste	Leitura	probe*		
ListMonitors	Concede permissão para listar todos os monitores em uma conta e seus status	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	monitor		
			probe		
TagResource	Concede permissão para adicionar tags da a um recurso	Marcação	monitor		
			probe		
UntagResource		Tags	monitor		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	Concede permissão para remover etiquetas de um recurso		probe		
				aws:TagKeys	
UpdateMonitor	Concede permissão para atualizar um monitor	Gravar	monitor*		
UpdateProbe	Concede permissão para atualizar um teste	Gravar	probe*		

Tipos de recursos definidos pelo Amazon CloudWatch Network Synthetic Monitor

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
monitor	`arn:${Partition}:networkmonitor:${Region}:${Account}:monitor/${MonitorName}`	aws:ResourceTag/${TagKey}
probe	`arn:${Partition}:networkmonitor:${Region}:${Account}:probe/${ProbeId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o Amazon CloudWatch Network Synthetic Monitor

O Amazon CloudWatch Network Synthetic Monitor define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso pelos pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o Amazon CloudWatch Observability Access Manager

O Amazon CloudWatch Observability Access Manager (prefixo do serviço:`oam`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon CloudWatch Observability Access Manager

- Tipos de recursos definidos pelo Amazon CloudWatch Observability Access Manager
- Chaves de condição para o Amazon CloudWatch Observability Access Manager

Ações definidas pelo Amazon CloudWatch Observability Access Manager

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateLink	Concede permissão para criar um link entre uma conta de monitoramento e uma conta de origem para monitoramento entre contas	Gravar	Sink*		oam:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys oam:ResourceTypes	
CreateSink	Concede permissão para criar um coletor em uma conta para que ele possa ser usado como uma conta de monitoramento para monitoramento entre contas	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	oam:TagResource
DeleteLink	Concede permissão para excluir um link entre uma conta de monitoramento e uma conta de origem para monitoramento entre contas	Gravar	Link*		
				aws:ResourceTag/${TagKey}	
DeleteSink	Concede permissão para excluir um coletor de	Gravar	Sink*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	monitoramento entre contas em uma conta de monitoramento			aws:ResourceTag/${TagKey}	
GetLink	Concede permissão para recuperar informações completas sobre um link de monitoramento entre contas	Leitura	Link*		
				aws:ResourceTag/${TagKey}	
GetSink	Concede permissão para recuperar informações completas sobre um coletor de monitoramento entre contas	Leitura	Sink*		
				aws:ResourceTag/${TagKey}	
GetSinkPolicy	Concede permissão para recuperar informações de política do IAM para um coletor de monitoramento entre contas	Leitura	Sink*		
				aws:ResourceTag/${TagKey}	
ListAttachedLinks	Concede permissão para recuperar uma lista de links vinculados para um coletor de monitoramento entre contas	Leitura	Sink*		
				aws:ResourceTag/${TagKey}	
ListLinks	Concede permissão para recuperar os links ARNs de monitoramento entre contas nesta conta	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListSinks	Concede permissão para recuperar os coletores ARNs de monitoramento de várias contas nesta conta	Leitura			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	Link		
			Sink		
PutSinkPolicy	Concede permissão para criar ou atualizar a política do IAM para um coletor de monitoramento entre contas	Gravar	Sink*		
				aws:ResourceTag/${TagKey}	
TagResource	Concede permissão para marcar um recurso	Marcação	Link		
			Sink		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso	Tags	Link		
			Sink		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateLink	Concede permissão para atualizar um link existente entre uma conta de monitoramento e uma conta de origem	Gravar	Link*		
				aws:ResourceTag/${TagKey} oam:ResourceTypes	

Tipos de recursos definidos pelo Amazon CloudWatch Observability Access Manager

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
Link	`arn:${Partition}:oam:${Region}:${Account}:link/${ResourceId}`	aws:ResourceTag/${TagKey}
Sink	`arn:${Partition}:oam:${Region}:${Account}:sink/${ResourceId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o Amazon CloudWatch Observability Access Manager

O Amazon CloudWatch Observability Access Manager define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves

para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString
oam:ResourceTypes	Filtra o acesso pela presença de tipos de recurso na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o Amazon CloudWatch Observability Admin Service

O Amazon CloudWatch Observability Admin Service (prefixo do serviço:`observabilityadmin`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon CloudWatch Observability Admin Service

- Tipos de recursos definidos pelo Amazon CloudWatch Observability Admin Service
- Chaves de condição para o Amazon CloudWatch Observability Admin Service

Ações definidas pelo Amazon CloudWatch Observability Admin Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateTelemetryRule	Concede permissão para criar uma nova regra de telemetria com o nome especificado para a conta	Gravar	telemetry-rule*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateTelemetryRuleForOrganization	Concede permissão para criar uma nova regra de telemetria da organização com o nome especificado para a organização	Gravar	organization-telemetry-rule*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteTelemetryRule	Concede permissão para excluir uma regra de telemetria com o nome especificado para a conta	Gravar	telemetry-rule*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteTelemetryRuleForOrganization	Concede permissão para excluir uma regra de telemetria da organização com o nome especificado para a organização	Gravar	organization-telemetry-rule*		
GetTelemetryEvaluationStatus	Concede permissão para recuperar o status do recurso de Configuração de Telemetria da conta	Leitura			
GetTelemetryEvaluationStatusForOrganization	Concede permissão para recuperar o status do recurso de Configuração de Telemetria para a organização	Leitura			
GetTelemetryRule	Concede permissão para recuperar a regra de telemetria especificada para a conta	Leitura			
GetTelemetryRuleForOrganization	Concede permissão para recuperar a regra de telemetria da organização especificada para a organização	Leitura			
ListResourceTelemetry	Concede permissão para recuperar configurações de telemetria para recursos associados à conta	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListResourceTelemetryForOrganization	Concede permissão para recuperar configurações de telemetria para recursos associados a contas na organização	Leitura			
ListTagsForResource	Concede permissão para listar as etiquetas para o recurso especificado	Lista	organization-telemetry-rule		
			telemetry-rule		
ListTelemetryRules	Concede permissão para listar as regras de telemetria da conta	Lista			
ListTelemetryRulesForOrganization	Concede permissão para listar as regras de telemetria da organização	Lista			
StartTelemetryEvaluation	Concede permissão para iniciar o recurso de Configuração de Telemetria para a conta	Gravar			
StartTelemetryEvaluationForOrganization	Concede permissão para iniciar o recurso de Configuração de Telemetria para a organização	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopTelemetryEvaluation	Concede permissão para interromper o recurso de Configuração de Telemetria da conta	Gravar			
StopTelemetryEvaluationForOrganization	Concede permissão para interromper o recurso de Configuração de Telemetria para a organização	Gravar			
TagResource	Concede permissão para adicionar ou atualizar as etiquetas especificadas no recurso especificado	Tags	organization-telemetry-rule		
			telemetry-rule		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover as etiquetas especificadas do recurso especificado	Tags	organization-telemetry-rule		
			telemetry-rule		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateTelemetryRule	Concede permissão para atualizar a regra de telemetria especificada para a conta	Gravar	telemetry-rule*		
UpdateTelemetryRuleForOrganization	Concede permissão para recuperar a regra de telemetria da organização especificada para a organização	Gravar	organization-telemetry-rule*		

Tipos de recursos definidos pelo Amazon CloudWatch Observability Admin Service

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
telemetry-rule	`arn:${Partition}:observabilityadmin:${Region}:${Account}:telemetry-rule:${TelemetryRuleName}`	aws:ResourceTag/${TagKey}
organization-telemetry-rule	`arn:${Partition}:observabilityadmin:${Region}:${Account}:organization-telemetry-rule:${TelemetryRuleName}`	aws:ResourceTag/${TagKey}

Chaves de condição para o Amazon CloudWatch Observability Admin Service

O Amazon CloudWatch Observability Admin Service define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para AWS CloudWatch RUM

AWS CloudWatch O RUM (prefixo do serviço:`rum`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS CloudWatch RUM
- Tipos de recursos definidos pelo AWS CloudWatch RUM

- Chaves de condição para AWS CloudWatch RUM

Ações definidas pelo AWS CloudWatch RUM

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchCreateRumMetricDefinitions	Concede permissão para criar as definições de métricas de rum	Gravar	AppMonitorResource*		
BatchDeleteRumMetricDefinitions	Concede permissão para remover as definições de métricas de rum	Gravar	AppMonitorResource*		
BatchGetRumMetricDefinitions	Concede permissão para obter as definições das métricas de rum	Leitura	AppMonitorResource*		
CreateAppMonitor	Concede permissão para criar metadados do appMonitor	Gravar	AppMonitorResource*		iam:CreateServiceLinkedRole iam:GetRole
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteAppMonitor	Concede permissão para excluir metadados do appMonitor	Gravar	AppMonitorResource*		
DeleteResourcePolicy	Concede permissão para excluir uma política de recursos anexada a um monitor de aplicativos	Gravar	AppMonitorResource*		
DeleteRumMetricsDestination	Concede permissão para excluir os destinos de métricas de rum	Gravar	AppMonitorResource*		
GetAppMonitor	Concede permissão para obter metadados do appMonitor	Leitura	AppMonitorResource*		
GetAppMonitorData	Concede permissão para obter dados do appMonitor	Leitura	AppMonitorResource*		
GetResourcePolicy	Concede permissão para recuperar uma política de recursos anexada a um monitor de aplicativos	Leitura	AppMonitorResource*		
ListAppMonitors	Concede permissão para listar metadados do appMonitors	Lista			
ListRumMetricsDestinations	Concede permissão para listar os destinos de métricas de rum	Leitura	AppMonitorResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar as etiquetas para recursos	Leitura			
PutResourcePolicy	Concede permissão para anexar uma política de recursos a um monitor de aplicativos	Gravar	AppMonitorResource*		
PutRumEvents	Concede permissão para colocar eventos RUM para appmonitor	Gravar	AppMonitorResource*		
PutRumMetricsDestination	Concede permissão para colocar os destinos de métricas de rum	Gravar	AppMonitorResource*		
TagResource	Concede permissão para marcar recursos	Tags	AppMonitorResource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar recursos	Tags	AppMonitorResource*		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateAppMonitor	Concede permissão para atualizar metadados do appmonitor	Gravar	AppMonitorResource*		iam:CreateServiceLinkedRole iam:GetRole
UpdateRumMetricDefinition	Concede permissão para atualizar a definição de métricas de rum	Gravar	AppMonitorResource*		

Tipos de recursos definidos pelo AWS CloudWatch RUM

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
AppMonitorResource	`arn:${Partition}:rum:${Region}:${Account}:appmonitor/${Name}`	aws:ResourceTag/${TagKey}

Chaves de condição para AWS CloudWatch RUM

AWS CloudWatch O RUM define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais

as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que fazem a solicitação em nome do primário do IAM	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso que fazem a solicitação em nome do primário do IAM	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação em nome do primário do IAM	ArrayOfString

Ações, recursos e chaves de condição para a Amazon CloudWatch Synthetics

O Amazon CloudWatch Synthetics (prefixo do serviço:`synthetics`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon CloudWatch Synthetics
- Tipos de recursos definidos pela Amazon CloudWatch Synthetics
- Chaves de condição para Amazon CloudWatch Synthetics

Ações definidas pela Amazon CloudWatch Synthetics

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateResource	Concede permissão para associar um recurso a um grupo	Gravar	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
CreateCanary	Concede permissão para criar um canary	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateGroup	Concede permissão para criar um grupo	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCanary	Concede permissão para excluir um canary. O Amazon Synthetics exclui todos os recursos, exceto a função Lambda e os alarmes, caso você tenha criado um. CloudWatch	Gravar	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteGroup	Concede permissão para excluir um grupo	Gravar	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
DescribeCanaries	Concede permissão para listar informações de todos os canaries	Read		synthetics:Names	
DescribeCanariesLastRun	Concede permissão para listar informações sobre a última execução de teste associada a todos os canaries	Read		synthetics:Names	
DescribeRuntimeVersions	Concede permissão para listar informações sobre versões de runtime canary do Synthetics.	Leitura			
DisassociateResource	Concede permissão para desassociar um recurso de um grupo	Gravar	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
GetCanary	Concede permissão para visualizar os detalhes de um canário	Leitura	canary*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:TagKeys	
GetCanaryRuns	Concede permissão para listar informações sobre todas as execuções de teste associadas a um canary	Leitura	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
GetGroup	Concede permissão para visualizar os detalhes de um grupo	Leitura	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ListAssociatedGroups	Concede permissão para listar informações sobre os grupos associados a um canário	Lista	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListGroupResources	Concede permissão para listar informações sobre canários em um grupo	Lista	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ListGroups	Concede permissão para listar informações de todos os grupos	Lista			
ListTagsForResource	Concede permissão para listar todas as tags e valores associados a um recurso	Leitura	canary		
			group		
StartCanary	Concede permissão para iniciar um canário, para que a Amazon CloudWatch Synthetics comece a monitorar um site	Gravar	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
StartCanaryDryRun	Concede permissão para iniciar uma operação a seco de canários, para que a Amazon CloudWatch Synthetics possa executar uma execução de teste de um canário com os parâmetros fornecidos	Gravar	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopCanary	Concede permissão para interromper um canary	Gravar	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
TagResource	Concede permissão para adicionar uma ou mais etiquetas a um recurso	Marcação	canary		
			group		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover uma ou mais etiquetas de um recurso	Tags	canary		
			group		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCanary	Concede permissão para atualizar um canary	Gravar	canary*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:TagKeys	

Tipos de recursos definidos pela Amazon CloudWatch Synthetics

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
canary	`arn:${Partition}:synthetics:${Region}:${Account}:canary:${CanaryName}`	aws:ResourceTag/${TagKey}
group	`arn:${Partition}:synthetics:${Region}:${Account}:group:${GroupId}`	aws:ResourceTag/${TagKey}

Chaves de condição para Amazon CloudWatch Synthetics

A Amazon CloudWatch Synthetics define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base nas etiquetas transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra as ações com base nas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra ações com base nas chaves da etiqueta transmitidas na solicitação	ArrayOfString
synthetics:Names	Filtra o acesso com base no nome do canary	ArrayOfString

Ações, recursos e chaves de condição para o AWS CodeArtifact

AWS CodeArtifact (prefixo do serviço:`codeartifact`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS CodeArtifact
- Tipos de recursos definidos pelo AWS CodeArtifact
- Chaves de condição do AWS CodeArtifact

Ações definidas pelo AWS CodeArtifact

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateExternalConnection	Concede permissão para adicionar uma conexão externa a um repositório	Write	repository*		
AssociateWithDownstreamRepository	Concede permissão para associar um repositório existente como um repositório upstream a outro repositório	Gravar	repository*		
CopyPackageVersions	Concede permissão para copiar versões de pacotes de um repositório para outro no mesmo domínio	Gravar	package* repository*		
CreateDomain	Concede permissão para criar um domínio	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePackageGroup	Concede permissão para criar um grupo de pacotes	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRepository	Concede permissão para criar um repositório	Write		aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
DeleteDomain	Concede permissão para excluir um domínio	Write	domain*		
DeleteDomainPermissionsPolicy	Concede permissão para excluir o conjunto de políticas de recursos em um domínio	Gerenciamento de permissões	domain*		
DeletePackage	Concede permissão para excluir um pacote	Gravar	package*		
DeletePackageGroup	Concede permissão para excluir um grupo de pacotes	Gravar	package-group*		
DeletePackageVersions	Concede permissão para excluir versões de pacote	Write	package*		
DeleteRepository	Concede permissão para excluir um repositório	Write	repository*		
DeleteRepositoryPermissionsPolicy	Concede permissão para excluir o conjunto de políticas de recursos em um repositório	Permissions management	repository*		
DescribeDomain	Concede permissão para retornar informações sobre um domínio	Leitura	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribePackage	Concede permissão para recuperar informações sobre um pacote	Leitura	package*		
DescribePackageGroup	Concede permissão para retornar informações detalhadas sobre um grupo de pacotes	Leitura	package-group*		
DescribePackageVersion	Concede permissão para retornar informações sobre uma versão de pacote	Read	package*		
DescribeRepository	Concede permissão para retornar informações detalhadas sobre um repositório	Read	repository*		
DisassociateExternalConnection	Concede permissão para desassociar uma conexão externa de um repositório	Write	repository*		
DisposePackageVersions	Concede permissão para definir o status de versões de pacote como Descartado e excluir os respectivos ativos	Gravar	package*		
GetAssociatedPackageGroup	Concede permissão para devolver o grupo de pacotes associado a um pacote	Leitura	package-group*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAuthorizationToken	Concede permissão para gerar um token de autenticação temporário para acessar repositórios em um domínio	Read	domain*		
GetDomainPermissionsPolicy	Concede permissão para retornar a política de recursos de um domínio	Read	domain*		
GetPackageVersionAsset	Concede permissão para retornar um ativo (ou arquivo) que faz parte de uma versão de pacote	Read	package*		
GetPackageVersionReadme	Concede permissão para retornar o arquivo readme de uma versão de pacote	Read	package*		
GetRepositoryEndpoint	Concede permissão para retornar um endpoint para um repositório	Read	repository*		
GetRepositoryPermissionsPolicy	Concede permissão para retornar a política de recursos de um repositório	Leitura	repository*		
ListAllowedRepositoriesForGroup	Concede permissão para listar os repositórios permitidos para um grupo de pacotes	Lista	package-group*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAssociatedPackages	Concede permissão para listar os pacotes associados a um grupo de pacotes	Lista	package-group*		
ListDomains	Concede permissão para listar os domínios no domínio do usuário atual Conta da AWS	Lista			
ListPackageGroups	Concede permissão para listar os grupos de pacotes em um domínio	Lista	domain*		
ListPackageVersionAssets	Concede permissão para listar os ativos de uma versão de pacote	List	package*		
ListPackageVersionDependencies	Concede permissão para listar as dependências diretas de uma versão de pacote	List	package*		
ListPackageVersions	Concede permissão para listar as versões de um pacote	List	package*		
ListPackages	Concede permissão para listar os pacotes em um repositório	List	repository*		
ListRepositories	Concede permissão para listar os repositórios administrados pela conta de chamada	List			
ListRepositoriesInDomain	Concede permissão para listar os repositórios em um domínio	Lista	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListSubPackageGroups	Concede permissão para listar os grupos de subpacotes de um grupo de pacotes principal	Lista	package-group*		
ListTagsForResource	Concede permissão para listar tags para um CodeArtifact recurso	Lista	domain		
			package-group		
			repository		
PublishPackageVersion	Concede permissão para publicar ativos e metadados em um endpoint de repositório	Write	package*		
PutDomainPermissionsPolicy	Concede permissão para anexar uma política de recursos a um domínio	Write	domain*		
PutPackageMetadata	Concede permissão para adicionar, modificar ou remover metadados de pacote usando um endpoint de repositório	Gravar	package*		
PutPackageOriginConfiguration	Concede permissão para definir a configuração de origem de um pacote	Gravar	package*		
PutRepositoryPermissionsPolicy	Concede permissão para anexar uma política de recursos a um repositório	Write	repository*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ReadFromRepository	Concede permissão para retornar ativos e metadados de pacote de um endpoint de repositório	Leitura	repository*		
TagResource	Concede permissão para marcar um CodeArtifact recurso	Tags	domain		
			package-group		
			repository		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover uma tag de um CodeArtifact recurso	Tags	domain		
			package-group		
			repository		
				aws:TagKeys	
UpdatePackageGroup	Concede permissão para modificar as propriedades de um grupo de pacotes	Gravar	package-group*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdatePackageGroupOriginConfiguration	Concede permissão para modificar a configuração de origem de pacotes de um grupo de pacotes	Gravar	package-group*		
UpdatePackageVersionsStatus	Concede permissão para modificar o status de uma ou mais versões de um pacote	Write	package*		
UpdateRepository	Concede permissão para modificar as propriedades de um repositório	Gravar	repository*		

Tipos de recursos definidos pelo AWS CodeArtifact

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

> **Note**
>
> O ARN do recurso de grupos de pacotes deve usar um padrão de grupo de pacotes codificado.

Tipos de recursos	ARN	Chaves de condição
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}`	

Chaves de condição do AWS CodeArtifact

AWS CodeArtifact define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para a Amazon CodeCatalyst

A Amazon CodeCatalyst (prefixo do serviço:`codecatalyst`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon CodeCatalyst
- Tipos de recursos definidos pela Amazon CodeCatalyst
- Chaves de condição para a Amazon CodeCatalyst

Ações definidas pela Amazon CodeCatalyst

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptConnection [somente permissão]	Concede permissão para aceitar uma solicitação para conectar essa conta a um CodeCatalyst espaço da Amazon	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
AssociateIamRoleToConnection [somente permissão]	Concede permissão para associar um perfil do IAM a uma conexão	Gravar	connections*		iam:PassRole
				aws:ResourceTag/${TagKey}	
AssociateIdentityCenterApplicationToSpace [somente permissão]	Concede permissão para associar um aplicativo do IAM Identity Center a um CodeCatalyst espaço da Amazon	Gravar	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
AssociateIdentityToIdentityCenterApplication [somente permissão]	Concede permissão para associar uma identidade a um aplicativo do IAM Identity Center para um CodeCatalyst espaço da Amazon	Gravar	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
BatchAssociateIden	Concede permissão para associar várias identidades a	Gravar	identity-center-ap		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
titiesToIdentityCenterApplication [somente permissão]	um aplicativo do IAM Identity Center para um espaço da Amazon CodeCatalyst		plications*		
				aws:ResourceTag/${TagKey}	
BatchDisassociateIdentitiesFromIdentityCenterApplication [somente permissão]	Concede permissão para desassociar várias identidades de um aplicativo do IAM Identity Center para um espaço da Amazon CodeCatalyst	Gravar	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
CreateIdentityCenterApplication [somente permissão]	Concede permissão para criar uma aplicação do IAM Identity Center	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSpace [somente permissão]	Concede permissão para criar um CodeCatalyst espaço na Amazon	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSpaceAdminRoleAssignment [somente permissão]	Concede permissão para criar uma atribuição de função de administrador para um determinado CodeCatalyst espaço da Amazon e aplicativo do IAM Identity Center	Gravar	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
DeleteConnection [somente permissão]	Concede permissão para excluir uma conexão	Gravar	connections*		
				aws:ResourceTag/${TagKey}	
DeleteIdentityCenterApplication [somente permissão]	Concede permissão para excluir uma aplicação do IAM Identity Center	Gravar	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
DisassociateIamRoleFromConnection [somente permissão]	Concede permissão para desassociar um perfil do IAM de uma conexão	Gravar	connections*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateIdentityCenterApplicationFromSpace [somente permissão]	Concede permissão para desassociar um aplicativo do IAM Identity Center de um espaço da Amazon CodeCatalyst	Gravar	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
DisassociateIdentityFromIdentityCenterApplication [somente permissão]	Concede permissão para desassociar uma identidade de um aplicativo do IAM Identity Center para um espaço da Amazon CodeCatalyst	Gravar	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
GetBillingAuthorization [somente permissão]	Concede permissão para descrever a autorização de cobrança para uma conexão	Leitura	connections*		
				aws:ResourceTag/${TagKey}	
GetConnection [somente permissão]	Concede permissão para obter uma conexão	Leitura	connections*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetIdentityCenterApplication [somente permissão]	Concede permissão para obter informações sobre uma aplicação do IAM Identity Center	Leitura	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
GetPendingConnection [somente permissão]	Concede permissão para receber uma solicitação pendente para conectar essa conta a um CodeCatalyst espaço da Amazon	Leitura			
ListConnections [somente permissão]	Concede permissão para listar conexões que não estejam pendentes	Lista			
ListIamRolesForConnection [somente permissão]	Concede permissão para listar perfis do IAM associados a uma conexão	Lista	connections*		
				aws:ResourceTag/${TagKey}	
ListIdentityCenterApplications [somente permissão]	Concede permissão para visualizar uma lista de todas as aplicações do IAM Identity Center na conta	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListIdentityCenterApplicationsForSpace [somente permissão]	Concede permissão para visualizar uma lista de aplicativos do IAM Identity Center por CodeCatalyst espaço da Amazon	Lista			
ListSpacesForIdentityCenterApplication [somente permissão]	Concede permissão para visualizar uma lista de CodeCatalyst espaços da Amazon pelo aplicativo IAM Identity Center	Lista	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource [somente permissão]	Concede permissão para listar tags para um CodeCatalyst recurso da Amazon	Leitura	connections		
			identity-center-applications		
				aws:ResourceTag/${TagKey}	
PutBillingAuthorization [somente permissão]	Concede permissão para criar ou atualizar a autorização de cobrança de uma conexão	Gravar	connections*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RejectConnection [somente permissão]	Concede permissão para rejeitar uma solicitação para conectar essa conta a um CodeCatalyst espaço da Amazon	Gravar			
SynchronizeIdentityCenterApplication [somente permissão]	Concede permissão para sincronizar uma aplicação do IAM Identity Center com o repositório de identidades de apoio	Gravar	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
TagResource [somente permissão]	Concede permissão para marcar um CodeCatalyst recurso da Amazon	Tags	connections		
			identity-center-applications		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource [somente permissão]	Concede permissão para desmarcar um recurso da Amazon CodeCatalyst	Tags	connections		
			identity-center-applications		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateIdentityCenterApplication [somente permissão]	Concede permissão para atualizar uma aplicação do IAM Identity Center	Gravar	identity-center-applications*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pela Amazon CodeCatalyst

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}`	

Chaves de condição para a Amazon CodeCatalyst

A Amazon CodeCatalyst define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso pela chave e valor de uma etiqueta em uma solicitação	String
aws:ResourceTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String

Chaves de condição	Descrição	Type
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta em uma solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS CodeCommit

AWS CodeCommit (prefixo do serviço:`codecommit`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS CodeCommit
- Tipos de recursos definidos pelo AWS CodeCommit
- Chaves de condição do AWS CodeCommit

Ações definidas pelo AWS CodeCommit

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateApprovalRuleTemplateWithRepository	Concede permissão para associar um modelo de regra de aprovação a um repositório	Write	repository*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchAssociateApprovalRuleTemplateWithRepositories	Concede permissão para associar um modelo de regra de aprovação a vários repositórios em uma única operação	Write	repository*		
BatchDescribeMergeConflicts	Concede permissão para obter informações sobre vários conflitos de mesclagem ao tentar mesclar duas confirmações usando a mesclagem de três vias ou a opção de mesclagem squash	Read	repository*		
BatchDisassociateApprovalRuleTemplateFromRepositories	Concede permissão para remover a associação entre um modelo de regra de aprovação e vários repositórios em uma única operação	Gravar	repository*		
BatchGetCommits	Concede permissão para retornar informações sobre um ou mais commits em um repositório AWS CodeCommit	Leitura	repository*		
BatchGetPullRequests [somente permissão]	Concede permissão para retornar informações sobre uma ou mais pull requests em um AWS CodeCommit repositório	Leitura	repository*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchGetRepositories	Concede permissão para obter informações sobre vários repositórios	Read	repository*		
CancelUploadArchive [somente permissão]	Concede permissão para cancelar o upload de um arquivo para um pipeline no AWS CodePipeline	Leitura	repository*		
CreateApprovalRuleTemplate	Concede permissão para criar um modelo de regra de aprovação que criará automaticamente regras de aprovação em solicitações pull que correspondam às condições definidas no modelo; não concede permissão para criar regras de aprovação para solicitações pull individuais	Gravar			
CreateBranch	Concede permissão para criar uma ramificação em um AWS CodeCommit repositório com essa API; não controla as ações de criação de ramificações do Git	Gravar	repository*		
				codecommit:References	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateCommit	Concede permissão para adicionar, copiar, mover ou atualizar um ou vários arquivos em uma ramificação em um AWS CodeCommit repositório e gerar um commit para as alterações na ramificação especificada	Gravar	repository*		
				codecommit:References	
CreatePullRequest	Concede permissão para criar uma solicitação pull no repositório especificado	Write	repository*		
CreatePullRequestApprovalRule	Concede permissão para criar uma regra de aprovação específica para uma solicitação pull individual; não concede permissão para criar modelos de regra de aprovação	Gravar	repository*		
CreateRepository	Concede permissão para criar um AWS CodeCommit repositório	Gravar	repository*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateUnreferencedMergeCommit	Concede permissão para criar uma confirmação não referenciada que contém o resultado da mesclagem de duas confirmações usando a opção de mesclagem de três vias ou squash; não controla ações de mesclagem do Git	Write	repository*		
				codecommit:References	
DeleteApprovalRuleTemplate	Concede permissão para excluir um modelo de regra de aprovação	Gravar			
DeleteBranch	Concede permissão para excluir uma ramificação em um AWS CodeCommit repositório com essa API; não controla as ações de exclusão de ramificações do Git	Gravar	repository*		
				codecommit:References	
DeleteCommentContent	Concede permissão para excluir o conteúdo de um comentário feito em uma alteração, um arquivo ou uma confirmação em um repositório	Write	repository*		
DeleteFile	Concede permissão para excluir um arquivo especificado de uma ramificação específica	Write	repository*		
				codecommit:References	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeletePullRequestApprovalRule	Concede permissão para excluir a regra de aprovação criada para uma solicitação pull se a regra não tiver sido criada por um modelo de regra de aprovação	Gravar	repository*		
DeleteRepository	Concede permissão para excluir um AWS CodeCommit repositório	Gravar	repository*		
DescribeMergeConflicts	Concede permissão para obter informações sobre conflitos de mesclagem específicos ao tentar mesclar duas confirmações usando a opção de mesclagem de três vias ou squash	Read	repository*		
DescribePullRequestEvents	Concede permissão para retornar informações sobre um ou mais eventos de solicitações pull	Read	repository*		
DisassociateApprovalRuleTemplateFromRepository	Concede permissão para remover a associação entre um modelo de regra de aprovação e um repositório	Write	repository*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
EvaluatePullRequestApprovalRules	Concede permissão para avaliar se uma solicitação pull é mesclável com base no estado atual de aprovação e nos requisitos da regra de aprovação	Read	repository*		
GetApprovalRuleTemplate	Concede permissão para retornar informações sobre um modelo de regra de aprovação	Leitura			
GetBlob	Concede permissão para visualizar o conteúdo codificado de um arquivo individual em um AWS CodeCommit repositório a partir do console AWS CodeCommit	Leitura	repository*		
GetBranch	Concede permissão para obter detalhes sobre uma ramificação em um AWS CodeCommit repositório com essa API; não controla as ações de ramificações do Git	Leitura	repository*		
GetComment	Concede permissão para obter o conteúdo de um comentário feito em uma alteração, um arquivo ou uma confirmação em um repositório	Read	repository*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetCommentReactions	Concede permissão para obter as reações em um comentário	Read	repository*		
GetCommentsForComparedCommit	Concede permissão para obter informações sobre comentários feitos na comparação entre duas confirmações	Read	repository*		
GetCommentsForPullRequest	Concede permissão para obter comentários feitos em uma solicitação pull	Read	repository*		
GetCommit	Concede permissão para retornar informações sobre uma confirmação, incluindo informações sobre a mensagem da confirmação e o responsável pela confirmação, com esta API. Não controla ações de log do Git	Read	repository*		
GetCommitHistory [somente permissão]	Concede permissão para obter informações sobre o histórico de confirmações em um repositório	Read	repository*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetCommitsFromMergeBase [somente permissão]	Concede permissão para obter informações sobre a diferença entre confirmações no contexto de uma possível mesclagem	Read	repository*		
GetDifferences	Concede permissão para visualizar informações sobre as diferenças entre os especificadores de confirmação válidos, como uma ramificação, uma etiqueta, um HEAD, um ID de confirmação ou outra referência totalmente qualificada	Read	repository*		
GetFile	Concede permissão para retornar o conteúdo codificado em base-64 de um arquivo especificado e seus metadados	Read	repository*		
GetFolder	Concede permissão para retornar o conteúdo de uma pasta especificada em um repositório	Read	repository*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetMergeCommit	Concede permissão para obter informações sobre uma confirmação de mesclagem criada por uma das opções de mesclagem para solicitações pull que criam confirmações de mesclagem. Nem todas as opções de mesclagem criam confirmações de mesclagem. Essa permissão não controla ações de mesclagem do Git	Leitura	repository*		
				codecommit:References	
GetMergeConflicts	Concede permissão para obter informações sobre conflitos de mesclagem entre a confirmação antes e depois IDs de uma pull request em um repositório	Leitura	repository*		
GetMergeOptions	Concede permissão para obter informações sobre opções de mesclagem de solicitações pull que podem ser usadas para mesclar duas confirmações; não controla ações de mesclagem do Git	Read	repository*		
GetObjectIdentifier [somente permissão]	Concede permissão para resolver blobs, árvores e confirmações ao respectivo identificador	Read	repository*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetPullRequest	Concede permissão para obter informações sobre uma solicitação pull em um repositório especificado	Read	repository*		
GetPullRequestApprovalStates	Concede permissão para recuperar as aprovações atuais em uma solicitação pull inserida	Read	repository*		
GetPullRequestOverrideState	Concede permissão para recuperar o estado de substituição atual de uma determinada solicitação pull	Read	repository*		
GetReferences [somente permissão]	Concede permissão para obter detalhes sobre referências em um AWS CodeCommit repositório; não controla as ações de referência do Git	Leitura	repository*		
GetRepository	Concede permissão para obter informações sobre um AWS CodeCommit repositório	Leitura	repository*		
GetRepositoryTriggers	Concede permissão para obter informações sobre triggers configurados para um repositório	Read	repository*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetTree [somente permissão]	Concede permissão para visualizar o conteúdo de uma árvore especificada em um AWS CodeCommit repositório a partir do console AWS CodeCommit	Leitura	repository*		
GetUploadArchiveStatus [somente permissão]	Concede permissão para obter informações de status sobre o upload de um arquivo para um pipeline no AWS CodePipeline	Leitura	repository*		
GitPull [somente permissão]	Concede permissão para extrair informações de um AWS CodeCommit repositório para um repositório local	Leitura	repository*		
GitPush [somente permissão]	Concede permissão para enviar informações de um repositório local para um AWS CodeCommit repositório	Gravar	repository*		
				codecommit:References	
ListApprovalRuleTemplates	Concede permissão para listar todos os modelos de regras de aprovação em um Região da AWS para o Conta da AWS	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAssociatedApprovalRuleTemplatesForRepository	Concede permissão para listar modelos de regra de aprovação associados a um repositório	Lista	repository*		
ListBranches	Concede permissão para listar ramificações para um AWS CodeCommit repositório com essa API; não controla as ações de ramificações do Git	Lista	repository*		
ListFileCommitHistory	Concede permissão para listar confirmações e alterações em um arquivo especificado	Lista	repository*		
ListPullRequests	Concede permissão para listar solicitações pull para um repositório especificado	Lista	repository*		
ListRepositories	Concede permissão para listar informações sobre AWS CodeCommit repositórios na região atual para seu Conta da AWS	Lista			
ListRepositoriesForApprovalRuleTemplate	Concede permissão para listar repositórios associados a um modelo de regra de aprovação	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar o recurso anexado a um ARN CodeCommit de recurso	Lista	repository		
MergeBranchesByFastForward	Concede permissão para mesclar duas confirmações especificadas na ramificação de destino usando a opção de mesclagem de avanço rápido	Write	repository*		
				codecommit:References	
MergeBranchesBySquash	Concede permissão para mesclar duas confirmações na ramificação de destino especificada usando a opção de mesclagem squash	Write	repository*		
				codecommit:References	
MergeBranchesByThreeWay	Concede permissão para mesclar duas confirmações na ramificação de destino especificada usando a opção de mesclagem de três vias	Write	repository*		
				codecommit:References	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
MergePullRequestByFastForward	Concede permissão para fechar uma solicitação pull e tentar mesclá-la com a ramificação de destino especificada para essa solicitação pull na confirmação especificada usando a opção de mesclagem de avanço rápido	Write	repository*		
				codecommit:References	
MergePullRequestBySquash	Concede permissão para fechar uma solicitação pull e tentar mesclá-la com a ramificação de destino especificada para essa solicitação pull na confirmação especificada usando a opção de mesclagem squash	Write	repository*		
				codecommit:References	
MergePullRequestByThreeWay	Concede permissão para fechar uma solicitação pull e tentar mesclá-la com a ramificação de destino especificada para essa solicitação pull na confirmação especificada usando a opção de mesclagem de três vias	Write	repository*		
				codecommit:References	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
OverridePullRequestApprovalRules	Concede permissão para substituir todas as regras de aprovação para uma solicitação pull, incluindo regras de aprovação criadas por um modelo	Write	repository*		
PostCommentForComparedCommit	Concede permissão para postar um comentário na comparação entre duas confirmações	Write	repository*		
PostCommentForPullRequest	Concede permissão para postar um comentário em uma solicitação pull	Write	repository*		
PostCommentReply	Concede permissão para postar um comentário em resposta a um comentário em uma comparação entre confirmações ou em uma solicitação pull	Write	repository*		
PutCommentReaction	Concede permissão para publicar uma reação em um comentário	Gravar	repository*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutFile	Concede permissão para adicionar ou atualizar um arquivo em uma ramificação em um AWS CodeCommit repositório e gerar um commit para a adição na ramificação especificada	Gravar	repository*		
				codecommit:References	
PutRepositoryTriggers	Concede permissão para criar, atualizar ou excluir triggers para um repositório	Gravar	repository*		
TagResource	Concede permissão para anexar tags de recursos a um ARN CodeCommit de recurso	Tags	repository		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
TestRepositoryTriggers	Concede permissão para testar a funcionalidade dos triggers do repositório enviando informações ao destino do trigger	Gravar	repository*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para desassociar tags de recursos de um ARN de CodeCommit recurso	Tags	repository		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateApprovalRuleTemplateContent	Concede permissão para atualizar o conteúdo dos modelos de regra de aprovação; não concede permissão para atualizar o conteúdo das regras de aprovação criadas especificamente para solicitações pull	Write			
UpdateApprovalRuleTemplateDescription	Concede permissão para atualizar a descrição dos modelos de regra de aprovação	Write			
UpdateApprovalRuleTemplateName	Concede permissão para atualizar o nome dos modelos de regra de aprovação	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateComment	Concede permissão para atualizar o conteúdo de um comentário se a identidade corresponder à identidade usada para criar o comentário	Gravar	repository*		
UpdateDefaultBranch	Concede permissão para alterar a ramificação padrão em um AWS CodeCommit repositório	Gravar	repository*		
UpdatePullRequestApprovalRuleContent	Concede permissão para atualizar o conteúdo das regras de aprovação criadas para solicitações pull específicas; não concede permissão para atualizar o conteúdo da regra de aprovação para regras criadas com um modelo de regra de aprovação	Write	repository*		
UpdatePullRequestApprovalState	Concede permissão para atualizar o estado de aprovação para solicitações pull	Write	repository*		
UpdatePullRequestDescription	Concede permissão para atualizar a descrição de uma solicitação pull	Write	repository*		
UpdatePullRequestStatus	Concede permissão para atualizar o status de uma solicitação pull	Write	repository*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdatePullRequestTitle	Concede permissão para atualizar o título de uma solicitação pull	Gravar	repository*		
UpdateRepositoryDescription	Concede permissão para alterar a descrição de um AWS CodeCommit repositório	Gravar	repository*		
UpdateRepositoryEncryptionKey	Concede permissão para alterar a chave de criptografia AWS KMS usada para criptografar e descriptografar um repositório AWS CodeCommit	Gravar	repository*		
UpdateRepositoryName	Concede permissão para alterar o nome de um AWS CodeCommit repositório	Gravar	repository*		
UploadArchive [somente permissão]	Concede permissão à função de serviço AWS CodePipeline para carregar alterações do repositório em um pipeline	Gravar	repository*		

Tipos de recursos definidos pelo AWS CodeCommit

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
repository	`arn:${Partition}:codecommit:${Region}:${Account}:${RepositoryName}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS CodeCommit

AWS CodeCommit define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString
codecommit:References	Filtra o acesso por referência do Git às ações especificadas AWS CodeCommit	String

Ações, recursos e chaves de condição para o AWS CodeConnections

AWS CodeConnections (prefixo do serviço:`codeconnections`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS CodeConnections
- Tipos de recursos definidos pelo AWS CodeConnections
- Chaves de condição do AWS CodeConnections

Ações definidas pelo AWS CodeConnections

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateConnection	Concede permissão para criar um recurso de conexão	Write		aws:RequestTag/${TagKey} aws:TagKeys codeconnections:ProviderType	
CreateHost	Concede permissão para criar um recurso de host	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				codeconnections:ProviderType codeconnections:VpcId	
CreateRepositoryLink	Concede permissão para criar um link de repositório	Gravar	Connection*		codeconnections:PassConnection codeconnections:UseConnection
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSyncConfiguration	Concede permissão para criar um modelo sync config	Gravar	RepositoryLink*		codeconnections:PassRepository iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				codeconnections:Branch	
DeleteConnection	Concede permissão para excluir um recurso de conexão	Write	Connection*		
DeleteHost	Concede permissão para excluir um recurso de host	Gravar	Host*		
DeleteRepositoryLink	Concede permissão para excluir um link de repositório	Gravar	RepositoryLink*		
DeleteSyncConfiguration	Concede permissão para excluir uma configuração de sincronização	Gravar			
GetConnection	Concede permissão para obter detalhes sobre um recurso de conexão	Leitura	Connection*		
GetConnectionToken [somente permissão]	Concede permissão para obter um token de conexão para chamar ações do provedor	Leitura	Connection*		
GetHost	Concede permissão para obter detalhes sobre um recurso de host	Read	Host*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetIndividualAccessToken [somente permissão]	Concede permissão para associar um terceiro, como uma instalação do aplicativo Bitbucket, a uma conexão	Read		codeconnections:ProviderType	codeconnections:StartOAuthHandshake
GetInstallationUrl [somente permissão]	Concede permissão para associar um terceiro, como uma instalação do aplicativo Bitbucket, a uma conexão	Leitura		codeconnections:ProviderType	
GetRepositoryLink	Concede permissão para descrever um link de repositório	Leitura	RepositoryLink*		
GetRepositorySyncStatus	Concede permissão para obter o status de sincronização mais recente de um repositório	Leitura	RepositoryLink*		
				codeconnections:Branch	
GetResourceSyncStatus	Concede permissão para obter o status de sincronização mais recente de um recurso (pilha cfn ou outros recursos)	Leitura			
GetSyncBlockerSummary	Concede permissão para descrever bloqueadores de sincronização de serviços de um recurso (pilha cfn ou outros recursos)	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSyncConfiguration	Concede permissão para descrever uma configuração de sincronização	Leitura			
ListConnections	Concede permissão para listar recursos de conexão	List	Connection*		
				codeconnections:ProviderTypeFilter	
ListHosts	Concede permissão para listar recursos de host	List		codeconnections:ProviderTypeFilter	
ListInstallationTargets [somente permissão]	Concede permissão para associar um terceiro, como uma instalação do aplicativo Bitbucket, a uma conexão	Lista			codeconnections:GetIndividualAccessToken codeconnections:StartOAuthHandshake
ListRepositoryLinks	Concede permissão para listar links de repositórios	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListRepositorySyncDefinitions	Concede permissão para listar definições de sincronização do repositório	Lista			
ListSyncConfigurations	Concede permissão para listar configurações de sincronização de um link de repositório	Lista			
ListTagsForResource	Concede permissão para definir o conjunto de pares chave/valor que são usados para gerenciar o recurso	Lista	Connection		
			Host		
			RepositoryLink		
PassConnection [somente permissão]	Concede permissão para passar um recurso de conexão para um AWS serviço que aceita um ARN de conexão como entrada, como codepipeline: CreatePipeline	Leitura	Connection*		
				codeconnections:PassedToService	
PassRepository [somente permissão]	Concede permissão para passar um recurso de link de repositório para um AWS serviço que aceita uma RepositoryLinkId como entrada, como codeconnections: CreateSyncConfiguration	Leitura	RepositoryLink*		
				codeconnections:PassedToService	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RegisterAppCode [somente permissão]	Concede permissão para associar um servidor de terceiros, como uma instância do GitHub Enterprise Server, a um Host	Leitura		codeconnections:HostArn	
StartAppRegistrationHandshake [somente permissão]	Concede permissão para associar um servidor de terceiros, como uma instância do GitHub Enterprise Server, a um Host	Leitura		codeconnections:HostArn	
StartOAuthHandshake [somente permissão]	Concede permissão para associar um terceiro, como uma instalação do aplicativo Bitbucket, a uma conexão	Leitura		codeconnections:ProviderType	
TagResource	Concede permissão para adicionar ou modificar as etiquetas do recurso especificado	Tags	Connection		
			Host		
			RepositoryLink		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para remover tags de um AWS recurso	Tags	Connection		
			Host		
			RepositoryLink		
				aws:TagKeys	
UpdateConnectionInstallation	Concede permissão para atualizar um recurso de conexão com uma instalação do aplicativo CodeStar Connections	Gravar	Connection*		codeconnections:GetIndividualAccessToken codeconnections:GetInstallationUrl codeconnections:ListInstallationTargets codeconnections:StartOAuthHandshake

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				codeconnections:InstallationId	
UpdateHost	Concede permissão para atualizar um recurso de host	Gravar	Host*		
				codeconnections:VpcId	
UpdateRepositoryLink	Concede permissão para atualizar um link de repositório	Gravar	RepositoryLink*		
UpdateSyncBlocker	Concede permissão para atualizar um bloqueador de sincronização para um recurso (cfn stack ou outros recursos)	Gravar			
UpdateSyncConfiguration	Concede permissão para atualizar uma configuração de sincronização	Gravar		codeconnections:Branch	
UseConnection [somente permissão]	Concede permissão para usar um recurso de conexão para chamar ações do provedor	Leitura	Connection*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				codeconnections:BranchName codeconnections:FullRepositoryId codeconnections:OwnerId codeconnections:ProviderAction codeconnections:ProviderPermissionsRequired codeconnections:RepositoryName	

Tipos de recursos definidos pelo AWS CodeConnections

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações

identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS CodeConnections

AWS CodeConnections define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString
codeconnections:Branch	Filtra o acesso pelo nome da ramificação que é passado na solicitação	String
codeconnections:BranchName	Filtra o acesso pelo nome da ramificação que é passado na solicitação. Aplica-se somente às UseConnection solicitações de acesso a uma ramificação específica do repositório	String
codeconnections:FullRepositoryId	Filtra o acesso pelo repositório que é passado na solicitação. Aplica-se somente às UseConnection solicitações de acesso a um repositório específico	String
codeconnections:HostArn	Filtra o acesso pelo recurso do host associado à conexão usada na solicitação	ARN
codeconnections:InstallationId	Filtra o acesso pelo ID de terceiros (como o ID de instalação do aplicativo Bitbucket para CodeConnections) que é usado para atualizar uma conexão. Permite restringir quais instalações de aplicativos de terceiros podem ser usadas para estabelecer uma conexão	String
codeconnections:OwnerId	Filtra o acesso pelo proprietário do repositório de terceiros. Aplica-se somente às UseConnection solicitações de acesso a repositórios pertencentes a um usuário específico	String
codeconnections:PassedToService	Filtra o acesso pelo serviço para o qual o principal tem permissão para passar uma conexão ou RepositoryLink	String

Chaves de condição	Descrição	Tipo
codeconnections:ProviderAction	Filtra o acesso pela ação do provedor em uma UseConnection solicitação, como ListRepositories. Consulte a documentação para todos os valores válidos	String
codeconnections:ProviderPermissionsRequired	Filtra o acesso pelas permissões de gravação de uma ação do provedor em uma UseConnection solicitação. Os tipos válidos incluem read_only e read_write	String
codeconnections:ProviderType	Filtra o acesso pelo tipo de provedor de terceiros passado na solicitação	String
codeconnections:ProviderTypeFilter	Filtra o acesso pelo tipo de provedor de terceiros usado para filtrar resultados	String
codeconnections:RepositoryName	Filtra o acesso pelo nome do repositório que é passado na solicitação. Aplica-se somente às UseConnection solicitações de acesso a repositórios pertencentes a um usuário específico	String
codeconnections:VpcId	Filtra o acesso pelo VpcId aprovado na solicitação	String

Ações, recursos e chaves de condição para o AWS CodeDeploy

AWS CodeDeploy (prefixo do serviço:`codedeploy`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.

- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS CodeDeploy
- Tipos de recursos definidos pelo AWS CodeDeploy
- Chaves de condição do AWS CodeDeploy

Ações definidas pelo AWS CodeDeploy

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddTagsToOnPremisesInstances	Concede permissão para adicionar etiquetas a uma ou mais instâncias on-premises	Tags	instance*		
BatchGetApplicationRevisions	Concede permissão para obter informações sobre uma ou mais revisões de aplicação	Leitura	application*		
BatchGetApplications	Concede permissão para obter informações sobre várias aplicações associadas ao usuário do IAM	Leitura	application*		
BatchGetDeploymentGroups	Concede permissão para obter informações sobre um ou mais grupos de implantação.	Leitura	deploymentgroup*		
BatchGetDeploymentInstances	Concede permissão para obter informações sobre uma ou mais instâncias que	Leitura	deploymentgroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	fazem parte de um grupo de implantações				
BatchGetDeploymentTargets	Concede permissão para retornar uma matriz de um ou mais destinos associados a uma implantação. Esse método funciona com todos os tipos de computação e deve ser usado em vez do obsoleto BatchGetDeploymentInstances. O número máximo de destinos que podem ser retornados é 25.	Leitura			
BatchGetDeployments	Concede permissão para obter informações sobre várias implantações associadas ao usuário do IAM	Leitura	deploymentgroup*		
BatchGetOnPremisesInstances	Concede permissão para obter informações sobre uma ou mais instâncias on-premises.	Leitura	instance*		
ContinueDeployment	Concede permissão para Iniciar o processo de redirecionamento do tráfego de instâncias no ambiente original para instâncias no ambiente de substituição sem esperar que ocorra um tempo de espera especificado	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateApplication	Concede permissão para criar uma aplicação associada ao usuário do IAM	Gravar	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudFormationDeployment [somente permissão]	Concede permissão para criar uma CloudFormation implantação para cooperar na orquestração de uma atualização de pilha CloudFormation	Gravar			
CreateDeployment	Concede permissão para criar uma implantação para uma aplicação associada ao usuário do IAM	Gravar	deploymentgroup*		
CreateDeploymentConfig	Concede permissão para criar uma configuração de implantação personalizada associada ao usuário do IAM	Gravar	deploymentconfig*		
CreateDeploymentGroup	Concede permissão para criar um grupo de implantação para uma aplicação associada ao usuário do IAM	Gravar	deploymentgroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Concede permissão para excluir uma aplicação associada ao usuário do IAM	Gravar	application*		
DeleteDeploymentConfig	Concede permissão para excluir uma configuração de implantação personalizada associada ao usuário do IAM	Gravar	deploymentconfig*		
DeleteDeploymentGroup	Concede permissão para excluir um grupo de implantação para uma aplicação associada ao usuário do IAM	Gravar	deploymentgroup*		
DeleteGitHubAccountToken	Concede permissão para excluir uma conexão de GitHub conta	Gravar			
DeleteResourcesByExternalId	Concede permissão para excluir recursos associados ao ID externo fornecido	Gravar			
DeregisterOnPremisesInstance	Concede permissão para cancelar o registro de uma instância on-premises	Gravar	instance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetApplication	Concede permissão para obter informações sobre uma única aplicação associada ao usuário do IAM	Lista	application*		
GetApplicationRevision	Concede permissão para obter informações sobre uma única revisão de aplicação para uma aplicação associada ao usuário do IAM	Lista	application*		
GetDeployment	Concede permissão para obter informações sobre uma única implantação em um grupo de implantações para uma aplicação associada ao usuário do IAM	Lista	deploymentgroup*		
GetDeploymentConfig	Concede permissão para obter informações sobre uma única configuração de implantação associada ao usuário do IAM	Lista	deploymentconfig*		
GetDeploymentGroup	Concede permissão para obter informações sobre um único grupo de implantações para uma aplicação associada ao usuário do IAM	Lista	deploymentgroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetDeploymentInstance	Concede permissão para obter informações sobre uma única instância em uma implantação associada ao usuário do IAM	Lista	deploymentgroup*		
GetDeploymentTarget	Concede permissão para retornar informações sobre um destino de implantação	Leitura			
GetOnPremisesInstance	Concede permissão para obter informações sobre uma única instância on-premises	Lista	instance*		
ListApplicationRevisions	Concede permissão para obter informações sobre todas as revisões de aplicação para uma aplicação associada ao usuário do IAM	Lista	application*		
ListApplications	Concede permissão para obter informações sobre todas as aplicações associadas ao usuário do IAM	Lista			
ListDeploymentConfigs	Concede permissão para obter informações sobre todas as configurações de implantação associadas ao usuário do IAM	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDeploymentGroups	Concede permissão para obter informações sobre todos os grupos de implantações para uma aplicação associada ao usuário do IAM	Lista	application*		
ListDeploymentInstances	Concede permissão para obter informações sobre todas as instâncias em uma implantação associada ao usuário do IAM	Lista	deploymentgroup*		
ListDeploymentTargets	Concede permissão para retornar uma matriz de IDs destinos associados a uma implantação	Lista			
ListDeployments	Concede permissão para obter informações sobre todas as implantações em um grupo de implantações associado ao usuário do IAM, ou obter todas as implantações associadas ao usuário do IAM	Lista	deploymentgroup*		
ListGitHubAccountTokenNames	Concede permissão para listar os nomes das conexões armazenadas GitHub nas contas	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListOnPremisesInstances	Concede permissão para obter uma lista de um ou mais nomes de instâncias on-premises	Lista			
ListTagsForResource	Concede permissão para retornar uma lista de etiquetas para o recurso identificado por um ARN especificado. As tags são usadas para organizar e categorizar seus recursos CodeDeploy	Lista	application deploymentgroup		
PutLifecycleEventHookExecutionStatus	Concede permissão para notificar um status de execução de hook de evento de ciclo de vida da implantação associada ao usuário do IAM	Gravar			
RegisterApplicationRevision	Concede permissão para registrar informações sobre uma revisão de uma aplicação associada ao usuário do IAM	Gravar	application*		
RegisterOnPremisesInstance	Concede permissão para registrar uma instância on-premises	Gravar	instance*		
RemoveTagsFromOnPremisesInstances	Concede permissão para remover etiquetas de uma ou mais instâncias on-premises	Tags	instance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SkipWaitTimeForInstanceTermination	Concede permissão para substituir qualquer tempo de espera especificado e inicia o encerramento de instâncias logo após a conclusão do roteamento de tráfego. Esta ação aplica-se somente às implantações azuis/verdes	Gravar			
StopDeployment	Concede permissão para interromper uma implantação	Gravar			
TagResource	Concede permissão para associar a lista de tags no parâmetro Tags de entrada ao recurso identificado pelo parâmetro ResourceArn de entrada	Tags	application		
			deploymentgroup		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para desassociar um recurso de uma lista de etiquetas. O recurso é identificado pelo parâmetro ResourceArn de entrada. As tags são identificadas pela lista de chaves no parâmetro de entrada TagKeys	Tags	application		
			deploymentgroup		
				aws:TagKeys	
UpdateApplication	Concede permissão para atualizar uma aplicação	Gravar	application*		
UpdateDeploymentGroup	Concede permissão para alterar informações sobre um único grupo de implantações para uma aplicação associada ao usuário do IAM	Gravar	deploymentgroup*		

Tipos de recursos definidos pelo AWS CodeDeploy

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}`	

Chaves de condição do AWS CodeDeploy

AWS CodeDeploy define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base na presença de pares de chave-valor da etiqueta na solicitação	String

Chaves de condição	Descrição	Type
aws:ResourceTag/${TagKey}	Filtra ações com base nos pares de chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações com base na presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o serviço AWS CodeDeploy seguro de comandos de host

AWS CodeDeploy O serviço secure host commands (prefixo do serviço:`codedeploy-commands-secure`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo serviço de comandos de host AWS CodeDeploy seguro
- Tipos de recursos definidos pelo serviço de comandos de host AWS CodeDeploy seguro
- Chaves de condição para serviço AWS CodeDeploy seguro de comandos de host

Ações definidas pelo serviço de comandos de host AWS CodeDeploy seguro

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetDeploymentSpecification	Concede permissão para obter uma especificação de implantação	Leitura			
PollHostCommand	Concede permissão para solicitar comandos do agente do host	Leitura			
PutHostCommandAcknowledgement	Concede permissão para marcar os comandos do agente do host reconhecidos	Gravar			
PutHostCommandComplete	Concede permissão para marcar os comandos do agente do host concluídos	Gravar			

Tipos de recursos definidos pelo serviço de comandos de host AWS CodeDeploy seguro

AWS CodeDeploy o serviço secure host commands não suporta a especificação de um ARN de recurso no elemento de uma `Resource` declaração de política do IAM. Para permitir o acesso ao serviço de comandos de host AWS CodeDeploy seguro, especifique `"Resource": "*"` em sua política.

Chaves de condição para serviço AWS CodeDeploy seguro de comandos de host

CodeDeploy O Commands Secure não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para a Amazon CodeGuru

A Amazon CodeGuru (prefixo do serviço:`codeguru`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon CodeGuru
- Tipos de recursos definidos pela Amazon CodeGuru
- Chaves de condição para a Amazon CodeGuru

Ações definidas pela Amazon CodeGuru

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetCodeGuruFreeTrialSummary [somente permissão]	Concede permissão para obter o resumo do teste gratuito do CodeGuru serviço, que inclui a data de validade	Leitura			

Tipos de recursos definidos pela Amazon CodeGuru

CodeGuru A Amazon não suporta a especificação de um ARN de recurso no elemento de uma `Resource` declaração de política do IAM. Para permitir o acesso à Amazon CodeGuru, especifique `"Resource": "*"` em sua política.

Chaves de condição para a Amazon CodeGuru

CodeGuru não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o Amazon CodeGuru Profiler

O Amazon CodeGuru Profiler (prefixo do serviço:`codeguru-profiler`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon CodeGuru Profiler
- Tipos de recursos definidos pelo Amazon CodeGuru Profiler
- Chaves de condição para o Amazon CodeGuru Profiler

Ações definidas pelo Amazon CodeGuru Profiler

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddNotificationChannels	Concede permissão para adicionar até 2 tópicos ARNs de tópicos existentes do AWS SNS para publicar notificações	Gravar	Profiling Group*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchGetFrameMetricData	Concede permissão para obter os dados de métrica de quadro para um grupo de criação de perfil	Lista	Profiling Group*		
ConfigureAgent	Concede permissão para registrar no serviço de orquestração e recuperar as informações de configuração de criação de perfil, usadas por agentes	Gravar	Profiling Group*		
CreateProfilingGroup	Concede permissão para criar um grupo de criação de perfil	Write		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteProfilingGroup	Concede permissão para excluir um grupo de criação de perfil	Write	Profiling Group*		
DescribeProfilingGroup	Concede permissão para descrever um grupo de criação de perfil	Read	Profiling Group*		
GetFindingsReportAccountSummary	Concede permissão para obter um resumo das recomendações recentes para cada grupo de criação de perfil na conta	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetNotificationConfiguration	Concede permissão para obter a configuração de notificação	Leitura	Profiling Group*		
GetPolicy	Concede permissão para obter a política de recursos associada ao grupo de criação de perfil especificado	Leitura	Profiling Group*		
GetProfile	Concede permissão para obter perfis agregados para um grupo de criação de perfil específico	Read	Profiling Group*		
GetRecommendations	Concede permissão para obter recomendações	Read	Profiling Group*		
ListFindingsReports	Concede permissão para listar os relatórios de recomendações disponíveis para um grupo de criação de perfil específico	List	Profiling Group*		
ListProfileTimes	Concede permissão para listar os horários de início dos perfis agregados disponíveis para um grupo de criação de perfil específico	List	Profiling Group*		
ListProfilingGroups	Concede permissão para listar grupos de criação de perfil na conta	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar etiquetas para um grupo de criação de perfil	Lista	Profiling Group*		
PostAgentProfile	Concede permissão para enviar um perfil coletado por um agente pertencente a um grupo de criação de perfil específico para agregação	Gravar	Profiling Group*		
PutPermission	Concede permissão para atualizar a lista de entidades principais permitidas para um grupo de ações na política de recursos associada ao grupo de criação de perfil especificado	Gerenciamento de permissões	Profiling Group*		
RemoveNotificationChannel	Concede permissão para excluir um SNStopic arn já configurado da configuração de notificação	Gravar	Profiling Group*		
RemovePermission	Concede permissão para remover a permissão do grupo de ações especificado da política de recursos associada ao grupo de criação de perfil especificado	Gerenciamento de permissões	Profiling Group*		
SubmitFeedback	Concede permissão para enviar feedback do usuário para anomalia útil ou não útil	Write	Profiling Group*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para adicionar ou substituir etiquetas para um grupo de criação de perfil	Marcação	Profiling Group*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover etiquetas de um grupo de criação de perfil	Marcação	Profiling Group*		
				aws:TagKeys	
UpdateProfilingGroup	Concede permissão para atualizar um grupo de criação de perfil específico	Gravar	Profiling Group*		

Tipos de recursos definidos pelo Amazon CodeGuru Profiler

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
Profiling Group	`arn:${Partition}:codeguru-profiler:${Region}:${Account}:profilingGroup/${ProfilingGroupName}`	aws:ResourceTag/${TagKey}

Chaves de condição para o Amazon CodeGuru Profiler

O Amazon CodeGuru Profiler define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o Amazon CodeGuru Reviewer

O Amazon CodeGuru Reviewer (prefixo do serviço:`codeguru-reviewer`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon CodeGuru Reviewer
- Tipos de recursos definidos pelo Amazon CodeGuru Reviewer
- Chaves de condição para Amazon CodeGuru Reviewer

Ações definidas pelo Amazon CodeGuru Reviewer

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de

condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
Associate Repository	Concede permissão para associar um repositório ao Amazon Reviewer CodeGuru	Gravar		aws:RequestTag/${TagKey}	codecommit:GetRepository
				aws:TagKeys	codecommit:ListRepositories
					codecommit:TagResource
					codestar-connections:PassConnection
					events:PutRule

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					events:PutTargets iam:CreateServiceLinkedRole s3:CreateBucket s3:ListBucket s3:PutBucketPolicy s3:PutLifecycleConfiguration
CreateCodeReview	Concede permissão para criar uma revisão de código	Write	association*		s3:GetObject
				aws:ResourceTag/${TagKey}	
CreateConnectionToken [somente permissão]	Concede permissão para executar handshake do OAuth baseado na Web para provedores de terceiros	Read			
DescribeCodeReview	Concede permissão para descrever uma revisão de código	Read	association*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
DescribeRecommendationFeedback	Concede permissão para descrever um comentário de recomendação sobre uma revisão de código	Read	association*		
				aws:ResourceTag/${TagKey}	
DescribeRepositoryAssociation	Concede permissão para descrever uma associação de repositório	Leitura	association*		
				aws:ResourceTag/${TagKey}	
DisassociateRepository	Concede permissão para desassociar um repositório do Amazon Reviewer CodeGuru	Gravar	association*		codecommit:UntagResource events:DeleteRule events:RemoveTargets
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetMetricsData [somente permissão]	Concede permissão para exibir métricas de solicitação pull no console	Read			
ListCodeReviews	Concede permissão para listar o resumo das revisões de código	List			
ListRecommendationFeedback	Concede permissão para listar o resumo dos comentários de recomendação em uma revisão de código	List	association*		
				aws:ResourceTag/${TagKey}	
ListRecommendations	Concede permissão para listar o resumo das recomendações em uma revisão de código	List	association*		
				aws:ResourceTag/${TagKey}	
ListRepositoryAssociations	Concede permissão para listar o resumo das associações de repositório	List			
ListTagsForResource	Concede permissão para listar o recurso vinculado a um ARN de repositório associado	List	association*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListThirdPartyRepositories [somente permissão]	Concede permissão para listar repositórios de provedores de terceiros no console	Read			
PutRecommendationFeedback	Concede permissão para colocar comentários para uma recomendação em uma revisão de código	Write	association*		
				aws:ResourceTag/${TagKey}	
TagResource	Concede permissão para associar etiquetas de recurso a um ARN de repositório associado	Marcação	association*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UnTagResource	Concede permissão para desassociar etiquetas de recurso de um ARN de repositório associado	Tags	association*		
				aws:TagKeys	

Tipos de recursos definidos pelo Amazon CodeGuru Reviewer

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações

identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
association	`arn:${Partition}:codeguru-reviewer:${Region}:${Account}:association:${ResourceId}`	aws:ResourceTag/${TagKey}
codereview	`arn:${Partition}:codeguru-reviewer:${Region}:${Account}:association:${ResourceId}:codereview:${CodeReviewId}`	

Chaves de condição para Amazon CodeGuru Reviewer

O Amazon CodeGuru Reviewer define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso com base na presença de pares de chave/valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra ações com base nos pares de chave-valor da etiqueta anexados ao recurso	String

Chaves de condição	Descrição	Type
aws:TagKeys	Filtra o acesso com base na presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para a Amazon CodeGuru Security

A Amazon CodeGuru Security (prefixo do serviço:`codeguru-security`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon CodeGuru Security
- Tipos de recursos definidos pela Amazon CodeGuru Security
- Chaves de condição para Amazon CodeGuru Security

Ações definidas pela Amazon CodeGuru Security

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchGetFindings	Concede permissão para recuperar em lote descobertas específicas geradas pela Segurança CodeGuru	Leitura	ScanName		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateScan	Concede permissão para criar uma verificação CodeGuru de segurança	Gravar	ScanName		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateUploadUrl	Concede permissão para gerar um URL pré-assinado para carregar arquivos de código	Gravar	ScanName		
DeleteScansByCategory [somente permissão]	Concede permissão para excluir todos os escaneamentos e descobertas relacionadas de CodeGuru Segurança por determinada categoria	Gravar			
GetAccountConfiguration	Concede permissão para recuperar as configurações no nível da conta	Leitura			
GetFindings	Concede permissão para recuperar descobertas de um escaneamento gerado pela Segurança CodeGuru	Lista	ScanName		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetMetricsSummary	Concede permissão para recuperar o resumo das métricas no nível AWS da conta gerado pela Segurança CodeGuru	Leitura			
GetScan	Concede permissão para recuperar metadados da verificação CodeGuru de segurança	Leitura	ScanName		
				aws:ResourceTag/${TagKey}	
ListFindings [somente permissão]	Concede permissão para recuperar descobertas geradas pela Security CodeGuru	Lista			
ListFindingsMetrics	Concede permissão para recuperar métricas de descobertas de nível de conta dentro de um intervalo de datas	Lista			
ListScans	Concede permissão para recuperar a lista de metadados da verificação de CodeGuru segurança	Lista			
ListTagsForResource	Concede permissão para recuperar uma lista de tags para um ARN de nome de verificação	Leitura	ScanName		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para adicionar tags para um ARN de nome de verificação	Tags	ScanName		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover tags de um ARN de nome de verificação	Tags	ScanName		
				aws:TagKeys	
UpdateAccountConfiguration	Concede permissão para atualizar as configurações de nível de conta	Gravar			

Tipos de recursos definidos pela Amazon CodeGuru Security

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
ScanName	`arn:${Partition}:codeguru-security:${Region}:${Account}:scans/${ScanName}`	aws:ResourceTag/${TagKey}

Chaves de condição para Amazon CodeGuru Security

A Amazon CodeGuru Security define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS CodePipeline

AWS CodePipeline (prefixo do serviço:`codepipeline`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS CodePipeline
- Tipos de recursos definidos pelo AWS CodePipeline
- Chaves de condição do AWS CodePipeline

Ações definidas pelo AWS CodePipeline

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de

condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcknowledgeJob	Concede permissão para visualizar informações sobre um trabalho especificado e indica se esse trabalho foi recebido pelo operador do trabalho.	Write			
AcknowledgeThirdPartyJob	Concede permissão para confirmar se um operador do trabalho recebeu o trabalho especificado (somente ações de parceiros)	Gravar			
CreateCustomActionType	Concede permissão para criar uma ação personalizada que você pode usar nos pipelines associados ao seu Conta da AWS	Gravar	actiontype*		
				aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
CreatePipeline	Concede permissão para criar um pipeline com nome exclusivo	Gravar	pipeline*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCustomActionType	Concede permissão para excluir uma ação personalizada	Write	actiontype*		
DeletePipeline	Concede permissão para excluir um pipeline especificado	Write	pipeline*		
DeleteWebhook	Concede permissão para excluir um webhook especificado	Write	webhook*		
DeregisterWebhookWithThirdParty	Concede permissão para remover o registro de um webhook com a terceira parte especificada em sua configuração	Write	webhook*		
DisableStageTransition	Concede permissão para impedir que as revisões façam transição para o próximo estágio em um pipeline.	Write	stage*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
EnableStageTransition	Concede permissão para permitir que as revisões façam transição para o próximo estágio em um pipeline	Gravar	stage*		
GetActionType	Concede permissão para visualizar informações sobre um tipo de ação	Leitura			
GetJobDetails	Concede permissão para visualizar informações sobre um trabalho (somente ações personalizadas)	Read			
GetPipeline	Concede permissão para recuperar informações sobre uma estrutura de pipeline	Read	pipeline*		
GetPipelineExecution	Concede permissão para visualizar informações sobre a execução de um pipeline, incluindo os detalhes sobre os artefatos, o ID de execução do pipeline e o nome, a versão e o status do pipeline	Read	pipeline*		
GetPipelineState	Concede permissão para visualizar informações sobre o estado atual dos estágios e das ações de um pipeline	Read	pipeline*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetThirdPartyJobDetails	Concede permissão para visualizar os detalhes de um trabalho para uma ação de terceiros (somente ações de parceiros)	Read			
ListActionExecutions	Concede permissão para listar as execuções de ações que ocorreram em um pipeline	Read	pipeline*		
ListActionTypes	Concede permissão para listar um resumo de todos os tipos de ação disponíveis para pipelines em sua conta	Leitura			
ListDeployActionExecutionTargets	Concede permissão para listar os detalhes de implantação para execuções de ações de implantação que ocorreram em um pipeline	Leitura	pipeline*		
ListPipelineExecutions	Concede permissão para listar um resumo das execuções mais recentes de um pipeline	Lista	pipeline*		
ListPipelines	Concede permissão para listar um resumo de todos os pipelines associados ao seu Conta da AWS	Lista			
ListRuleExecutions	Concede permissão para listar as execuções de regras que ocorreram em um pipeline	Leitura	pipeline*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListRuleTypes	Concede permissão para listar um resumo de todos os tipos de regra disponíveis para pipelines em sua conta	Leitura			
ListTagsForResource	Concede permissão para listar tags para um CodePipeline recurso	Leitura	actiontype		
			pipeline		
			webhook		
ListWebhooks	Concede permissão para listar todos os webhooks associados ao seu Conta da AWS	Lista	webhook*		
OverrideStageCondition	Concede permissão para retomar a execução do pipeline ao substituir uma condição em um estágio	Gravar	stage*		
PollForJobs	Concede permissão para visualizar informações sobre quaisquer trabalhos CodePipeline nos quais atuar	Gravar	actiontype*		
PollForThirdPartyJobs	Concede permissão para determinar se há trabalhos de terceiros para um operador de trabalho atuar nele (somente ações de parceiros)	Write			
PutActionRevision	Concede permissão para editar ações em um pipeline	Gravar	action*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutApprovalResult	Concede permissão para fornecer uma resposta (aprovada ou rejeitada) a uma solicitação de aprovação manual no CodePipeline	Gravar	action*		
PutJobFailureResult	Concede permissão para representar a falha de um trabalho como retornado ao pipeline por um operador de trabalho (somente ações personalizadas)	Write			
PutJobSuccessResult	Concede permissão para representar o sucesso de um trabalho conforme retornado ao pipeline por um operador de trabalho (somente ações personalizadas)	Write			
PutThirdPartyJobFailureResult	Concede permissão para representar a falha de um trabalho de terceiros conforme retornado ao pipeline por um operador de trabalho (somente ações de parceiros)	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutThirdPartyJobSuccessResult	Concede permissão para representar o sucesso de um trabalho de terceiros conforme retornado ao pipeline por um operador de trabalho (somente ações de parceiros)	Write			
PutWebhook	Concede permissão para criar ou atualizar um webhook	Gravar	pipeline*		
			webhook*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RegisterWebhookWithThirdParty	Concede permissão para registrar um webhook com a terceira parte especificada em sua configuração.	Write	webhook*		
RetryStageExecution	Concede permissão para retomar a execução do pipeline ao recuperar as últimas ações com falha em um estágio.	Gravar	stage*		
RollbackStage	Concede permissão para reverter o estágio a uma execução anterior bem-sucedida	Gravar	stage*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartPipelineExecution	Concede permissão para executar a revisão mais recente por meio do pipeline	Write	pipeline*		
StopPipelineExecution	Concede permissão para interromper uma execução de pipeline em andamento	Gravar	pipeline*		
TagResource	Concede permissão para marcar um CodePipeline recurso	Tags	actiontype		
			pipeline		
			webhook		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover uma tag de um CodePipeline recurso	Tags	actiontype		
			pipeline		
			webhook		
				aws:TagKeys	
UpdateActionType	Concede permissão para atualizar um tipo de ação	Gravar	actiontype*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdatePipeline	Concede permissão para atualizar um pipeline com alterações na estrutura do pipeline.	Gravar	pipeline*		

Tipos de recursos definidos pelo AWS CodePipeline

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
webhook	`arn:${Partition}:codepipeline:${Region}:${Account}:webhook:${WebhookName}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS CodePipeline

AWS CodePipeline define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base na presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra ações com base nos pares de chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações com base na presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS CodeStar

AWS CodeStar (prefixo do serviço:`codestar`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS CodeStar
- Tipos de recursos definidos pelo AWS CodeStar
- Chaves de condição do AWS CodeStar

Ações definidas pelo AWS CodeStar

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de

condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateTeamMember	Concede permissão para adicionar um usuário à equipe de um AWS CodeStar projeto	Gerenciamento de permissões	project*		
CreateProject	Concede permissão para criar um projeto com estrutura e políticas de cliente mínimas e nenhum recurso	Gerenciamento de permissões		aws:RequestTag/${TagKey} aws:TagKeys	
CreateUserProfile	Concede permissão para criar um perfil de usuário contendo preferências do usuário, nome de exibição e e-mail	Gravar	user*		
DeleteExtendedAcce	Concede permissão para exclusão estendida APIs	Gravar	project*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ss [somente permissão]					
DeleteProject	Concede permissão para excluir um projeto, inclusive os recursos do projeto. Não exclui os usuários associados ao projeto, mas exclui os perfis do IAM que permitiam acesso ao projeto	Gerenciamento de permissões	project*		
DeleteUserProfile	Concede permissão para excluir um perfil de usuário em AWS CodeStar, incluindo todos os dados de preferências pessoais associados a esse perfil, como nome de exibição e endereço de e-mail. Não exclui o histórico desse usuário, por exemplo, o histórico de confirmações feitas pelo usuário	Gravar	user*		
DescribeProject	Concede permissão para descrever um projeto e seus recursos	Leitura	project*		
DescribeUserProfile	Concede permissão para descrever um usuário em AWS CodeStar e os atributos do usuário em todos os projetos	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateTeamMember	Concede permissão para remover um usuário de um projeto. A remoção de um usuário de um projeto também remove as políticas do IAM desse usuário que permitiam acessar o projeto e seus recursos	Gerenciamento de permissões	project*		
GetExtendedAccess [somente permissão]	Concede permissão para leitura estendida APIs	Leitura	project*		
ListProjects	Concede permissão para listar todos os projetos CodeStar associados ao seu Conta da AWS	Lista			
ListResources	Concede permissão para listar todos os recursos associados a um projeto no CodeStar	Lista	project*		
ListTagsForProject	Concede permissão para listar as tags associadas a um projeto no CodeStar	Lista	project*		
ListTeamMembers	Concede permissão para listar todos os membros da equipe associados a um projeto	Lista	project*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListUserProfiles	Concede permissão para listar perfis de usuário no AWS CodeStar	Lista			
PutExtendedAccess [somente permissão]	Concede permissão para escrita estendida APIs	Gravar	project*		
TagProject	Concede permissão para adicionar tags a um projeto no CodeStar	Tags	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagProject	Concede permissão para remover tags de um projeto no CodeStar	Tags	project*		
				aws:TagKeys	
UpdateProject	Concede permissão para atualizar um projeto no CodeStar	Gravar	project*		
UpdateTeamMember	Concede permissão para atualizar os atributos dos membros da equipe em um CodeStar projeto	Gerenciamento de permissões	project*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateUserProfile	Concede permissão para atualizar um perfil de usuário contendo preferências do usuário, nome de exibição e e-mail	Gravar	user*		
VerifyServiceRole	Concede permissão para verificar se a função de AWS CodeStar serviço existe na conta do cliente	Lista			

Tipos de recursos definidos pelo AWS CodeStar

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
project	`arn:${Partition}:codestar:${Region}:${Account}:project/${ProjectId}`	aws:ResourceTag/${TagKey}
user	`arn:${Partition}:iam::${Account}:user/${AwsUserName}`	iam:ResourceTag/${TagKey}

Chaves de condição do AWS CodeStar

AWS CodeStar define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por solicitações com base no conjunto de valores permitido para cada uma das etiquetas	String
aws:ResourceTag/${TagKey}	Filtra o acesso por ações com base na etiqueta-valor associada ao recurso	String
aws:TagKeys	Filtra o acesso para solicitações com base na presença de etiquetas obrigatórias na solicitação	ArrayOfString
iam:ResourceTag/${TagKey}	Filtra o acesso por ações com base na etiqueta-valor associada ao recurso	String

Ações, recursos e chaves de condição para AWS CodeStar conexões

AWS CodeStar As conexões (prefixo do serviço:`codestar-connections`) fornecem os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas por AWS CodeStar Conexões
- Tipos de recursos definidos por AWS CodeStar Conexões
- Chaves de condição para AWS CodeStar conexões

Ações definidas por AWS CodeStar Conexões

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateConnection	Concede permissão para criar um recurso de conexão	Write		aws:RequestTag/${TagKey} aws:TagKeys codestar-connections:ProviderType	
CreateHost	Concede permissão para criar um recurso de host	Gravar		aws:RequestTag/${TagKey} aws:TagKeys codestar-connectio	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ns:ProviderType codestar-connections:VpcId	
CreateRepositoryLink	Concede permissão para criar um link de repositório	Gravar	Connection*		codestar-connections:PassConnection codestar-connections:UseConnection
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSyncConfiguration	Concede permissão para criar um modelo sync config	Gravar	RepositoryLink*		codestar-connections:PassRepository iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				codestar-connections:Branch	
DeleteConnection	Concede permissão para excluir um recurso de conexão	Write	Connection*		
DeleteHost	Concede permissão para excluir um recurso de host	Gravar	Host*		
DeleteRepositoryLink	Concede permissão para excluir um link de repositório	Gravar	RepositoryLink*		
DeleteSyncConfiguration	Concede permissão para excluir uma configuração de sincronização	Gravar			
GetConnection	Concede permissão para obter detalhes sobre um recurso de conexão	Leitura	Connection*		
GetConnectionToken [somente permissão]	Concede permissão para obter um token de conexão para chamar ações do provedor	Leitura	Connection*		
GetHost	Concede permissão para obter detalhes sobre um recurso de host	Read	Host*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetIndividualAccessToken [somente permissão]	Concede permissão para associar um terceiro, como uma instalação do aplicativo Bitbucket, a uma conexão	Read		codestar-connections:ProviderType	codestar-connections:StartOAuthHandshake
GetInstallationUrl [somente permissão]	Concede permissão para associar um terceiro, como uma instalação do aplicativo Bitbucket, a uma conexão	Leitura		codestar-connections:ProviderType	
GetRepositoryLink	Concede permissão para descrever um link de repositório	Leitura	RepositoryLink*		
GetRepositorySyncStatus	Concede permissão para obter o status de sincronização mais recente de um repositório	Leitura	RepositoryLink*		
				codestar-connections:Branch	
GetResourceSyncStatus	Concede permissão para obter o status de sincronização mais recente de um recurso (pilha cfn ou outros recursos)	Leitura			
GetSyncBlockerSummary	Concede permissão para descrever bloqueadores de sincronização de serviços de um recurso (pilha cfn ou outros recursos)	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSyncConfiguration	Concede permissão para descrever uma configuração de sincronização	Leitura			
ListConnections	Concede permissão para listar recursos de conexão	List	Connection*		
				codestar-connections:ProviderTypeFilter	
ListHosts	Concede permissão para listar recursos de host	List		codestar-connections:ProviderTypeFilter	
ListInstallationTargets [somente permissão]	Concede permissão para associar um terceiro, como uma instalação do aplicativo Bitbucket, a uma conexão	Lista			codestar-connections:GetIndividualAccessToken codestar-connections:StartOAuthHandshake
ListRepositoryLinks	Concede permissão para listar links de repositórios	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListRepositorySyncDefinitions	Concede permissão para listar definições de sincronização do repositório	Lista			
ListSyncConfigurations	Concede permissão para listar configurações de sincronização de um link de repositório	Lista			
ListTagsForResource	Concede permissão para definir o conjunto de pares chave/valor que são usados para gerenciar o recurso	Lista	Connection		
			Host		
			RepositoryLink		
PassConnection [somente permissão]	Concede permissão para passar um recurso de conexão para um AWS serviço que aceita um ARN de conexão como entrada, como codepipeline: CreatePipeline	Leitura	Connection*		
				codestar-connections:PassedToService	
PassRepository [somente permissão]	Concede permissão para passar um recurso de link de repositório para um AWS serviço que aceita uma RepositoryLinkId como entrada, como codestar-connections: CreateSyncConfiguration	Leitura	RepositoryLink*		
				codestar-connections:PassedToService	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RegisterAppCode [somente permissão]	Concede permissão para associar um servidor de terceiros, como uma instância do GitHub Enterprise Server, a um Host	Leitura		codestar-connections:HostArn	
StartAppRegistrationHandshake [somente permissão]	Concede permissão para associar um servidor de terceiros, como uma instância do GitHub Enterprise Server, a um Host	Leitura		codestar-connections:HostArn	
StartOAuthHandshake [somente permissão]	Concede permissão para associar um terceiro, como uma instalação do aplicativo Bitbucket, a uma conexão	Leitura		codestar-connections:ProviderType	
TagResource	Concede permissão para adicionar ou modificar as etiquetas do recurso especificado	Tags	Connection		
			Host		
			RepositoryLink		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para remover tags de um AWS recurso	Tags	Connection		
			Host		
			RepositoryLink		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateConnectionInstallation	Concede permissão para atualizar um recurso de conexão com uma instalação do aplicativo CodeStar Connections	Gravar	Connection*		codestar-connections:GetIndividualAccessToken codestar-connections:GetInstallationUrl codestar-connections:ListInstallationTargets codestar-connections:StartOAuthHandshake
				codestar-connections:InstallationId	
UpdateHost	Concede permissão para atualizar um recurso de host	Gravar	Host*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				codestar-connections:VpcId	
UpdateRepositoryLink	Concede permissão para atualizar um link de repositório	Gravar	RepositoryLink*		
UpdateSyncBlocker	Concede permissão para atualizar um bloqueador de sincronização para um recurso (cfn stack ou outros recursos)	Gravar			
UpdateSyncConfiguration	Concede permissão para atualizar uma configuração de sincronização	Gravar		codestar-connections:Branch	
UseConnection [somente permissão]	Concede permissão para usar um recurso de conexão para chamar ações do provedor	Leitura	Connection*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				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 Conexões

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição para AWS CodeStar conexões

AWS CodeStar As conexões definem as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString
codestar-connections:Branch	Filtra o acesso pelo nome da ramificação que é passado na solicitação	String
codestar-connections:BranchName	Filtra o acesso pelo nome da ramificação que é passado na solicitação. Aplica-se somente às UseConnection solicitações de acesso a uma ramificação específica do repositório	String
codestar-connections:FullRepositoryId	Filtra o acesso pelo repositório que é passado na solicitação. Aplica-se somente às UseConnection solicitações de acesso a um repositório específico	String
codestar-connections:HostArn	Filtra o acesso pelo recurso do host associado à conexão usada na solicitação	ARN
codestar-connections:InstallationId	Filtra o acesso pela ID de terceiros (como a ID de instalação do aplicativo Bitbucket para CodeStar conexões) usada para atualizar uma conexão. Permite restringir quais instalações de aplicativos de terceiros podem ser usadas para estabelecer uma conexão	String

Chaves de condição	Descrição	Tipo
codestar-connections:OwnerId	Filtra o acesso pelo proprietário do repositório de terceiros. Aplica-se somente às UseConnection solicitações de acesso a repositórios pertencentes a um usuário específico	String
codestar-connections:PassedToService	Filtra o acesso pelo serviço para o qual o principal tem permissão para passar uma conexão ou RepositoryLink	String
codestar-connections:ProviderAction	Filtra o acesso pela ação do provedor em uma UseConnection solicitação, como ListRepositories. Consulte a documentação para todos os valores válidos	String
codestar-connections:ProviderPermissionsRequired	Filtra o acesso pelas permissões de gravação de uma ação do provedor em uma UseConnection solicitação. Os tipos válidos incluem read_only e read_write	String
codestar-connections:ProviderType	Filtra o acesso pelo tipo de provedor de terceiros passado na solicitação	String
codestar-connections:ProviderTypeFilter	Filtra o acesso pelo tipo de provedor de terceiros usado para filtrar resultados	String
codestar-connections:RepositoryName	Filtra o acesso pelo nome do repositório que é passado na solicitação. Aplica-se somente às UseConnection solicitações de acesso a repositórios pertencentes a um usuário específico	String

Chaves de condição	Descrição	Tipo
codestar-connections:VpcId	Filtra o acesso pelo VpcId aprovado na solicitação	String

Ações, recursos e chaves de condição para AWS CodeStar notificações

AWS CodeStar As notificações (prefixo do serviço:`codestar-notifications`) fornecem os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelas AWS CodeStar notificações
- Tipos de recursos definidos por AWS CodeStar Notificações
- Teclas de condição para AWS CodeStar notificações

Ações definidas pelas AWS CodeStar notificações

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o

nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateNotificationRule	Concede permissão para criar uma regra de notificação para um recurso	Write	notificationrule*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	
DeleteNotificationRule	Concede permissão para excluir uma regra de notificação de um recurso	Write	notificationrule*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	
DeleteTarget	Concede permissão para excluir um destino de uma regra de notificação	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DescribeNotificationRule	Concede permissão para obter informações sobre uma regra de notificação	Read	notificationrule*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	
ListEventTypes	Concede permissão para listar tipos de eventos de notificações	Lista			
ListNotificationRules	Concede permissão para listar regras de notificação em um Conta da AWS	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas anexadas a um ARN de recurso de regra de notificação	Lista	notificationrule*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
ListTargets	Concede permissão para listar os alvos da regra de notificação para um Conta da AWS	Lista		aws:RequestTag/${TagKey} aws:TagKeys	
Subscribe	Concede permissão para criar uma associação entre uma regra de notificação e um tópico do Amazon SNS	Write	notificationrule*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para anexar etiquetas de recurso a um ARN de recurso de regra de notificação	Marcação	notificationrule*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
Unsubscribe	Concede permissão para remover uma associação entre uma regra de notificação e um tópico do Amazon SNS	Write	notificationrule*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para desassociar etiquetas de recurso de um ARN de recurso de regra de notificação	Marcação	notificationrule*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateNotificationRule	Concede permissão para alterar uma regra de notificação para um recurso	Gravar	notificationrule*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	

Tipos de recursos definidos por AWS CodeStar Notificações

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
notificationrule	`arn:${Partition}:codestar-notifications:${Region}:${Account}:notificationrule/${NotificationRuleId}`	aws:ResourceTag/${TagKey}

Teclas de condição para AWS CodeStar notificações

AWS CodeStar As notificações definem as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base na presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra ações com base nos pares de chave-valor da etiqueta anexados ao recurso	String

Chaves de condição	Descrição	Type
aws:TagKeys	Filtra ações com base na presença de chaves da etiqueta na solicitação	ArrayOfString
codestar-notifications:NotificationsForResource	Filtra o acesso com base no ARN do recurso para o qual as notificações estão configuradas	ARN

Ações, recursos e chaves de condição para a Amazon CodeWhisperer

A Amazon CodeWhisperer (prefixo do serviço:`codewhisperer`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon CodeWhisperer
- Tipos de recursos definidos pela Amazon CodeWhisperer
- Chaves de condição para a Amazon CodeWhisperer

Ações definidas pela Amazon CodeWhisperer

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AllowVendedLogDeliveryForResource [somente permissão]	Concede permissão para configurar a entrega de registros vendidos para o recurso de CodeWhisperer personalização	Gerenciamento de permissões	customization*		
				aws:ResourceTag/${TagKey}	
AssociateCustomizationPermission [somente permissão]	Concede permissão para invocar AssociateCustomizationPermission em CodeWhisperer	Gravar	customization*		
				aws:ResourceTag/${TagKey}	
CreateCustomization [somente permissão]	Concede permissão para invocar CreateCustomization em CodeWhisperer	Gravar	customization*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateProfile [somente permissão]	Concede permissão para invocar CreateProfile em CodeWhisperer	Gravar	profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteCustomization [somente permissão]	Concede permissão para invocar DeleteCustomization em CodeWhisperer	Gravar	customization*		
				aws:ResourceTag/${TagKey}	
DeleteProfile [somente permissão]	Concede permissão para invocar DeleteProfile em CodeWhisperer	Gravar	profile*		
				aws:ResourceTag/${TagKey}	
DisassociateCustomizationPermission [somente permissão]	Concede permissão para invocar DisassociateCustomizationPermission em CodeWhisperer	Gravar	customization*		
				aws:ResourceTag/${TagKey}	
GenerateRecommendations [somente permissão]	Concede permissão para invocar GenerateRecommendations em CodeWhisperer	Leitura			
GetCustomization [somente permissão]	Concede permissão para invocar GetCustomization em CodeWhisperer	Leitura	customization*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListCustomizationPermissions [somente permissão]	Concede permissão para invocar ListCustomizationPermissions em CodeWhisperer	Lista	customization*		
				aws:ResourceTag/${TagKey}	
ListCustomizationVersions [somente permissão]	Concede permissão para invocar ListCustomizationVersions em CodeWhisperer	Lista	customization*		
				aws:ResourceTag/${TagKey}	
ListCustomizations [somente permissão]	Concede permissão para invocar ListCustomizations em CodeWhisperer	Lista	customization*		
ListProfiles [somente permissão]	Concede permissão para invocar ListProfiles em CodeWhisperer	Lista			
ListTagsForResource [somente permissão]	Concede permissão para invocar ListTagsForResource em CodeWhisperer	Lista	customization		
			profile		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource [somente permissão]	Concede permissão para invocar TagResource em CodeWhisperer	Tags	customization		
			profile		
				aws:ResourceTag/${TagKey} aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [somente permissão]	Concede permissão para invocar UntagResource em CodeWhisperer	Tags	customization		
			profile		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCustomization [somente permissão]	Concede permissão para invocar UpdateCustomization em CodeWhisperer	Gravar	customization*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateProfile [somente permissão]	Concede permissão para invocar UpdateProfile em CodeWhisperer	Gravar	profile*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pela Amazon CodeWhisperer

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
profile	`arn:${Partition}:codewhisperer:${Region}:${Account}:profile/${Identifier}`	aws:ResourceTag/${TagKey}
customization	`arn:${Partition}:codewhisperer:${Region}:${Account}:customization/${Identifier}`	aws:ResourceTag/${TagKey}

Chaves de condição para a Amazon CodeWhisperer

A Amazon CodeWhisperer define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais

as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas tags associadas ao CodeWhisperer recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Cognito Identity

O Amazon Cognito Identity (prefixo do serviço: `cognito-identity`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Cognito Identity
- Tipos de recursos definidos pelo Amazon Cognito Identity
- Chaves de condição do Amazon Cognito Identity

Ações definidas pelo Amazon Cognito Identity

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateIdentityPool	Concede permissão para criar um novo pool de identidades	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteIdentities	Concede permissão para excluir identidades de um pool de identidades. Você pode especificar uma lista de 1-60 identidades que deseja excluir	Write			
DeleteIdentityPool	Concede permissão para excluir um pool de usuários. Após um pool ser excluído, os usuários não poderão se autenticar nele.	Write	identitypool*		
DescribeIdentity	Concede permissão para retornar metadados relacionados à identidade dada, inclusive quando a identidade foi criada e quaisquer logins vinculados associados	Read			
DescribeIdentityPool	Concede permissão para obter detalhes sobre um determinado pool de identidades, incluindo o nome do pool, a descrição do ID, a data de	Read	identitypool*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	criação e o número atual de usuários				
GetCredentialsForIdentity	Concede permissão para retornar credenciais para o ID de identidade fornecido	Read			
GetId	Concede permissão para gerar (ou recuperar) um ID do Cognito. O fornecimento de vários logins criará uma conta vinculada implícita	Gravar			
GetIdentityPoolAnalytics	Concede permissão para obter dados analíticos sobre a contagem total de identidades atual de todos os provedores de identidade do pool de identidades (IdPs)	Leitura	identitypool*		
GetIdentityPoolDailyAnalytics	Concede permissão para obter dados analíticos sobre o número de novas identidades e o total de identidades para todos os provedores de identidade do pool de identidades () IdPs	Leitura	identitypool*		
GetIdentityPoolRoles	Concede permissão para obter as funções de um pool de identidades	Leitura	identitypool*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetIdentityProviderDailyAnalytics	Concede permissão para obter dados analíticos sobre o número de novas identidades e o total de identidades de um provedor de identidade do grupo de identidades () IdPs	Leitura	identitypool*		
GetOpenIdToken	Concede permissão para obter um token OpenID, usando um ID conhecido do Cognito	Leitura			
GetOpenIdTokenForDeveloperIdentity	Concede permissão para registrar (ou recuperar) um token do IdentityId Cognito e do OpenID Connect para um usuário autenticado pelo seu processo de autenticação de back-end	Leitura	identitypool*		
GetPrincipalTagAttributeMap	Concede permissão para obter as principais etiquetas para um pool de identidades e provedor	Read	identitypool*		
ListIdentities	Concede permissão para listar as identidades de um pool de identidades	List	identitypool*		
ListIdentityPools	Concede permissão para listar todos os pools de identidades do Cognito registrados na sua conta	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar as etiquetas atribuídas a um pool de identidades do Amazon Cognito	Leitura	identitypool		
LookupDeveloperIdentity	Concede permissão para recuperar o IdentityId associado a uma Developer UserIdentifier ou a lista de DeveloperUserIdentifiers associados a uma IdentityId para uma identidade existente	Leitura	identitypool*		
MergeDeveloperIdentities	Concede permissão para mesclar dois usuários diferentes IdentityIds, existentes no mesmo grupo de identidades e identificados pelo mesmo provedor de desenvolvedores	Gravar	identitypool*		
SetIdentityPoolRoles	Concede permissão para definir as funções para um pool de identidades. Essas funções são usadas ao fazer chamadas à GetCredentialsForIdentity ação.	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SetPrincipalTagAttributeMap	Concede permissão para definir as principais etiquetas para um pool de identidades e provedor. Essas tags são usadas ao fazer chamadas à GetOpenIdToken ação.	Gravar			
TagResource	Concede permissão para atribuir um conjunto de etiquetas a um pool de identidades do Amazon Cognito	Tags	identitypool		
				aws:RequestTag/${TagKey} aws:TagKeys	
UnlinkDeveloperIdentity	Concede permissão para desvincular Developer UserIdentifier a de uma identidade existente	Gravar	identitypool*		
UnlinkIdentity	Concede permissão para desvincular uma identidade federada de uma conta existente	Write			
UntagResource	Concede permissão para remover as etiquetas especificadas de um pool de identidades do Amazon Cognito	Marcação	identitypool		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateIdentityPool	Concede permissão para atualizar um pool de identidades	Write	identitypool*		

Tipos de recursos definidos pelo Amazon Cognito Identity

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
identitypool	`arn:${Partition}:cognito-identity:${Region}:${Account}:identitypool/${IdentityPoolId}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Cognito Identity

O Amazon Cognito Identity define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base na presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra ações com base nos pares de chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso por uma chave presente na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Cognito Sync

O Amazon Cognito Sync (prefixo do serviço: `cognito-sync`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Cognito Sync
- Tipos de recursos definidos pelo Amazon Cognito Sync
- Chaves de condição do Amazon Cognito Sync

Ações definidas pelo Amazon Cognito Sync

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BulkPublish	Concede permissão para iniciar uma publicação em massa de todos os conjuntos de dados existentes para um grupo de identidades no fluxo configurado	Gravar	identitypool*		
DeleteDataset	Concede permissão para excluir um conjunto de dados específico	Gravar	dataset*		
DescribeDataset	Concede permissão para obter metadados sobre um conjunto de dados por identidade e nome do conjunto de dados	Leitura	dataset*		
DescribeIdentityPoolUsage	Concede permissão para obter detalhes de uso (por exemplo, armazenamento físico de dados) sobre determinado grupo de identidades	Leitura	identitypool*		
DescribeIdentityUsage	Concede permissão para obter informações de uso de uma identidade, inclusive o número de conjuntos de dados e o uso dos dados	Leitura	identity*		
GetBulkPublishDetails	Concede permissão para obter o status da última	Leitura	identitypool*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	BulkPublish operação de um grupo de identidades				
GetCognitoEvents	Concede permissão para obter os eventos e as funções Lambda correspondentes associados a um grupo de identidades	Leitura	identitypool*		
GetIdentityPoolConfiguration	Concede permissão para obter as configurações de um grupo de identidades	Leitura	identitypool*		
ListDatasets	Concede permissão para listar conjuntos de dados para uma identidade	Lista	dataset*		
ListIdentityPoolUsage	Concede permissão para obter uma lista com todos os grupos de identidades registrados com o Cognito	Leitura	identitypool*		
ListRecords	Concede permissão para obter os registros paginados, opcionalmente alterados depois de determinada contagem de sincronização de um conjunto de dados e identidade	Leitura	dataset*		
QueryRecords [somente permissão]	Concede permissão para consultar registros	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RegisterDevice	Concede permissão para registrar um dispositivo para receber notificações de sincronização por push	Gravar	identity*		
SetCognitoEvents	Concede permissão para definir a função AWS Lambda para um determinado tipo de evento para um grupo de identidades	Gravar	identitypool*		
SetDatasetConfiguration [somente permissão]	Concede permissão para configurar conjuntos de dados	Gravar	dataset*		
SetIdentityPoolConfiguration	Concede permissão para definir a configuração necessária para a sincronização por push	Gravar	identitypool*		
SubscribeToDataset	Concede permissão para assinar para receber notificações quando um conjunto de dados é modificado por outro dispositivo	Gravar	dataset*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UnsubscribeFromDataset	Concede permissão para cancelar a assinatura para receber notificações quando um conjunto de dados é modificado por outro dispositivo	Gravar	dataset*		
UpdateRecords	Concede permissão para publicar atualizações feitas em registros e para adicionar e excluir registros de um conjunto de dados e usuário	Gravar	dataset*		

Tipos de recursos definidos pelo Amazon Cognito Sync

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
dataset	`arn:${Partition}:cognito-sync:${Region}:${Account}:identitypool/${IdentityPoolId}/identity/${IdentityId}/dataset/${DatasetName}`	

Tipos de recursos	ARN	Chaves de condição
identity	`arn:${Partition}:cognito-sync:${Region}:${Account}:identitypool/${IdentityPoolId}/identity/${IdentityId}`	
identitypool	`arn:${Partition}:cognito-sync:${Region}:${Account}:identitypool/${IdentityPoolId}`	

Chaves de condição do Amazon Cognito Sync

O Cognito Sync não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição dos grupos de usuários do Amazon Cognito

Os Grupos de usuários do Amazon Cognito (prefixo do serviço: `cognito-idp`) fornecem os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelos grupos de usuários do Amazon Cognito
- Tipos de recursos definidos pelos grupos de usuários do Amazon Cognito
- Chaves de condição dos grupos de usuários do Amazon Cognito

Ações definidas pelos grupos de usuários do Amazon Cognito

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddCustomAttributes	Concede permissão para adicionar atributos de usuário ao esquema do grupo de usuários	Gravar	userpool*		
AdminAddUserToGroup	Concede permissão para adicionar qualquer usuário a qualquer grupo	Gravar	userpool*		
AdminConfirmSignUp	Concede permissão para confirmar o registro de qualquer usuário sem um código de confirmação	Gravar	userpool*		
AdminCreateUser	Concede permissão para criar novos usuários e enviar mensagens de boas-vindas por e-mail ou SMS	Gravar	userpool*		
AdminDeleteUser	Concede permissão para excluir qualquer usuário	Gravar	userpool*		
AdminDeleteUserAttributes	Concede permissão para excluir atributos de qualquer usuário	Gravar	userpool*		
AdminDisableProviderForUser	Concede permissão para desvincular qualquer usuário do grupo de usuários de um usuário de provedor de identidades (IdP) terceirizado	Gravar	userpool*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AdminDisableUser	Concede permissão para desativar qualquer usuário	Gravar	userpool*		
AdminEnableUser	Concede permissão para ativar qualquer usuário	Gravar	userpool*		
AdminForgetDevice	Concede permissão para cancelar o registro de dispositivos de qualquer usuário	Gravar	userpool*		
AdminGetDevice	Concede permissão para obter informações sobre os dispositivos de qualquer usuário	Leitura	userpool*		
AdminGetUser	Concede permissão para pesquisar qualquer usuário por nome de usuário	Leitura	userpool*		
AdminInitiateAuth	Concede permissão para autenticar qualquer usuário	Gravar	userpool*		
AdminLinkProviderForUser	Concede permissão para vincular qualquer usuário do grupo de usuários de um usuário provedor de identidades (IdP) terceirizado	Gravar	userpool*		
AdminListDevices	Concede permissão para listar os dispositivos lembrados de qualquer usuário	Lista	userpool*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AdminListGroupsForUser	Concede permissão para listar os grupos aos quais qualquer usuário pertence	Lista	userpool*		
AdminListUserAuthEvents	Concede permissão para listar eventos de login para qualquer usuário	Leitura	userpool*		
AdminRemoveUserFromGroup	Concede permissão para remover qualquer usuário de qualquer grupo	Gravar	userpool*		
AdminResetUserPassword	Concede permissão para redefinir a senha de qualquer usuário	Gravar	userpool*		
AdminRespondToAuthChallenge	Concede permissão para responder a um desafio de autenticação durante a autenticação de qualquer usuário	Gravar	userpool*		
AdminSetUserMFAPreference	Concede permissão para definir o método de MFA preferido de qualquer usuário	Gravar	userpool*		
AdminSetUserPassword	Concede permissão para definir a senha de qualquer usuário	Gravar	userpool*		
AdminSetUserSettings	Concede permissão para definir configurações de usuário para qualquer usuário	Gravar	userpool*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AdminUpdateAuthEventFeedback	Concede permissão para atualizar o feedback de segurança avançada para evento de autenticação de qualquer usuário	Gravar	userpool*		
AdminUpdateDeviceStatus	Concede permissão para atualizar o status dos dispositivos lembrados de qualquer usuário	Gravar	userpool*		
AdminUpdateUserAttributes	Concede permissão para atualizar os atributos padrão ou personalizados de qualquer usuário	Gravar	userpool*		
AdminUserGlobalSignOut	Concede permissão para desconectar qualquer usuário de todas as sessões	Gravar	userpool*		
AssociateSoftwareToken	Concede permissão para retornar um código de chave secreta compartilhada gerado de forma exclusiva para o usuário	Gravar			
AssociateWebACL [somente permissão]	Concede permissão para associar o grupo de usuários a uma Web ACL AWS do WAF	Gravar	userpool* webacl*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ChangePassword	Concede permissão para alterar a senha de um usuário especificado em um grupo de usuários	Gravar			
ConfirmDevice	Concede permissão para confirmar o rastreamento do dispositivo. Essa chamada de API é a chamada que inicia o rastreamento do dispositivo	Gravar			
ConfirmForgotPassword	Concede permissão para que um usuário insira um código de confirmação para redefinir uma senha esquecida	Gravar			
ConfirmSignUp	Concede permissão para confirmar o registro de um usuário e manipula o alias existente de um usuário anterior	Gravar			
CreateGroup	Concede permissão para criar novos grupos de usuários	Gravar	userpool*		
CreateIdentityProvider	Concede permissão para adicionar provedores de identidades aos grupos de usuários	Gravar	userpool*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateManagedLoginBranding	Concede permissão para criar configurações de identidade visual para login gerenciado e associá-las a um cliente de aplicativo	Gravar	userpool*		
CreateResourceServer	Concede permissão para criar e configurar escopos para servidores de recursos OAuth 2.0	Gravar	userpool*		
CreateUserImportJob	Concede permissão para criar trabalhos de importação de CSV do usuário	Gravar	userpool*		
CreateUserPool	Concede permissão para criar e definir política de senha para grupos de usuários	Gravar		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateUserPoolClient	Concede permissão para criar clientes de aplicação de grupo de usuários	Gravar	userpool*		
CreateUserPoolDomain	Concede permissão para adicionar domínios de grupo de usuário	Gravar	userpool*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteGroup	Concede permissão para excluir qualquer grupo de usuários vazio	Gravar	userpool*		
DeleteIdentityProvider	Concede permissão para excluir qualquer provedor de identidades de grupos de usuários	Gravar	userpool*		
DeleteManagedLoginBranding	Concede permissão para excluir o estilo de marca de login gerenciado para qualquer cliente de aplicativo	Gravar	userpool*		
DeleteResourceServer	Concede permissão para excluir qualquer servidor de recursos OAuth 2.0 dos grupos de usuários	Gravar	userpool*		
DeleteUser	Concede permissão para permitir que um usuário exclua a si mesmo	Gravar			
DeleteUserAttributes	Concede permissão para excluir os atributos de um usuário	Gravar			
DeleteUserPool	Concede permissão para excluir grupos de usuários	Gravar	userpool*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteUserPoolClient	Concede permissão para excluir qualquer cliente de aplicação de grupo de usuários	Gravar	userpool*		
DeleteUserPoolDomain	Concede permissão para excluir qualquer domínio de grupo de usuários	Gravar	userpool*		
DescribeIdentityProvider	Concede permissão para descrever qualquer provedor de identidades de grupo de usuários	Leitura	userpool*		
DescribeManagedLoginBranding	Concede permissão para obter informações detalhadas sobre o estilo de marca do login gerenciado	Leitura	userpool*		
DescribeManagedLoginBrandingByClient	Concede permissão para obter informações detalhadas sobre o estilo de marca do login gerenciado associado a um aplicativo/cliente.	Leitura	userpool*		
DescribeResourceServer	Concede permissão para descrever qualquer servidor de recursos OAuth 2.0	Leitura	userpool*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeRiskConfiguration	Concede permissão para descrever as definições de configuração de risco de grupos de usuários e clientes de aplicações	Leitura	userpool*		
DescribeUserImportJob	Concede permissão para descrever qualquer trabalho de importação de usuário	Leitura	userpool*		
DescribeUserPool	Concede permissão para descrever grupos de usuários	Leitura	userpool*		
DescribeUserPoolClient	Concede permissão para descrever qualquer cliente de aplicação de grupo de usuários	Leitura	userpool*		
DescribeUserPoolDomain	Concede permissão para descrever qualquer domínio de grupo de usuários	Leitura			
DisassociateWebACL [somente permissão]	Concede permissão para desassociar o grupo de usuários com uma Web ACL do AWS WAF	Gravar	userpool*		
ForgetDevice	Concede permissão para esquecer o dispositivo especificado	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ForgotPassword	Concede permissão para enviar uma mensagem ao usuário final com um código de confirmação que é necessário para alterar a senha do usuário	Gravar			
GetCSVHeader	Concede permissão para gerar cabeçalhos para um arquivo .csv de importação de usuário	Leitura	userpool*		
GetDevice	Concede permissão para obter o dispositivo	Leitura			
GetGroup	Concede permissão para descrever um grupo de usuários	Leitura	userpool*		
GetIdentityProviderByIdentifier	Concede permissão para correlacionar um identificador de IdP de grupo de usuários ao nome do IdP	Leitura	userpool*		
GetLogDeliveryConfiguration	Concede permissão para obter a configuração detalhada do log de atividades para um grupo de usuários	Leitura	userpool*		
GetSigningCertificate	Concede permissão para pesquisar certificados de assinatura para grupos de usuários	Leitura	userpool*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetTokensFromRefreshToken	Concede permissão para atualizar tokens de usuário com tokens de atualização	Gravar			
GetUICustomization	Concede permissão para obter informações de personalização da interface de usuário para a interface de usuário hospedada de qualquer cliente de aplicação	Leitura	userpool*		
GetUser	Concede permissão para obter os atributos e metadados de um usuário	Leitura			
GetUserAttributeVerificationCode	Concede permissão para obter o código de verificação do atributo do usuário para o nome do atributo especificado	Leitura			
GetUserPoolMfaConfig	Concede permissão para pesquisar a configuração de MFA de grupos de usuários	Leitura	userpool*		
GetWebACLForResource [somente permissão]	Concede permissão para obter a ACL web do AWS WAF associada a um grupo de usuários do Amazon Cognito	Leitura	userpool*		
GlobalSignOut	Concede permissão para desconectar usuários de todos os dispositivos	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
InitiateAuth	Concede permissão para iniciar o fluxo de autenticação	Gravar			
ListDevices	Concede permissão para listar os dispositivos	Lista			
ListGroups	Concede permissão para listar todos os grupos em grupos de usuários	Lista	userpool*		
ListIdentityProviders	Concede permissão para listar todos os provedores de identidades nos grupos de usuários	Lista	userpool*		
ListResourceServers	Concede permissão para listar todos os servidores de recursos em grupos de usuários	Lista	userpool*		
ListResourcesForWebACL [somente permissão]	Concede permissão para listar os grupos de usuários associados a uma Web ACL AWS do WAF	Lista	webacl*		
ListTagsForResource	Concede permissão para listar as tags atribuídas a um grupo de usuários do Amazon Cognito	Lista	userpool		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListUserImportJobs	Concede permissão para listar todos os trabalhos de importação de usuário	Lista	userpool*		
ListUserPoolClients	Concede permissão para listar todos os clientes de aplicação em grupos de usuários	Lista	userpool*		
ListUserPools	Concede permissão para listar todos os grupos de usuários	Lista			
ListUsers	Concede permissão para listar todos os usuários de grupo de usuários	Lista	userpool*		
ListUsersInGroup	Concede permissão para listar os usuários em qualquer grupo	Lista	userpool*		
ResendConfirmationCode	Concede permissão para reenviar a confirmação (para confirmação do registro) a um usuário específico no grupo de usuários	Gravar			
RespondToAuthChallenge	Concede permissão para responder ao desafio de autenticação	Gravar			
RevokeToken	Concede permissão para revogar todos os tokens de acesso gerados pelo token de atualização especificado	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SetLogDeliveryConfiguration	Concede permissão para configurar ou modificar a configuração detalhada do log de atividades para um grupo de usuários	Gravar	userpool*		
SetRiskConfiguration	Concede permissão para definir a configuração de risco para grupos de usuários e clientes de aplicações	Gravar	userpool*		
SetUICustomization	Concede permissão para personalizar a interface do usuário hospedada para qualquer cliente de aplicação	Gravar	userpool*		
SetUserMFAPreference	Concede permissão para definir a preferência de MFA para o usuário no grupo de usuários	Gravar			
SetUserPoolMfaConfig	Concede permissão para definir a configuração de MFA de um grupo de usuários	Gravar	userpool*		
SetUserSettings	Concede permissão para definir configurações do usuário, como a autenticação multifator (MFA)	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SignUp	Concede permissão para registrar o usuário no grupo de usuários especificado e cria um nome de usuário, uma senha e atributos de usuário	Gravar			
StartUserImportJob	Concede permissão para iniciar qualquer trabalho de importação de usuário	Gravar	userpool*		
StopUserImportJob	Concede permissão para interromper qualquer trabalho de importação de usuário	Gravar	userpool*		
TagResource	Concede permissão para marcar um grupo de usuários	Tags	userpool		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um grupo de usuários	Tags	userpool		
				aws:TagKeys	
UpdateAuthEventFeedback	Concede permissão para atualizar os comentários do evento de autenticação de usuário	Gravar	userpool*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateDeviceStatus	Concede permissão para atualizar o status do dispositivo	Gravar			
UpdateGroup	Concede permissão para atualizar a configuração de qualquer grupo	Gravar	userpool*		
UpdateIdentityProvider	Concede permissão para atualizar a configuração de IdP de qualquer grupo de usuários	Gravar	userpool*		
UpdateManagedLoginBranding	Concede permissão para atualizar as configurações de identidade visual de um login gerenciado	Gravar	userpool*		
UpdateResourceServer	Concede permissão para atualizar a configuração de qualquer servidor de recursos OAuth 2.0	Gravar	userpool*		
UpdateUserAttributes	Concede permissão para o usuário atualizar um atributo específico (um de cada vez)	Gravar			
UpdateUserPool	Concede permissão para atualizar a configuração de grupos de usuários	Gravar	userpool*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateUserPoolClient	Concede permissão para atualizar qualquer cliente de grupo de usuários	Gravar	userpool*		
UpdateUserPoolDomain	Concede permissão para substituir o certificado para qualquer domínio personalizado	Gravar	userpool*		
VerifySoftwareToken	Concede permissão para registrar o código da TOTP inserido de um usuário e marcar o status de MFA de token de software do usuário como verificado, em caso de êxito	Gravar			
VerifyUserAttribute	Concede permissão para verificar um atributo do usuário usando um código de verificação único	Gravar			

Tipos de recursos definidos pelos grupos de usuários do Amazon Cognito

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações

identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
userpool	`arn:${Partition}:cognito-idp:${Region}:${Account}:userpool/${UserPoolId}`	aws:ResourceTag/${TagKey}
webacl	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/webacl/${Name}/${Id}`	

Chaves de condição dos grupos de usuários do Amazon Cognito

Os Grupos de usuários do Amazon Cognito definem as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso por uma chave presente na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Comprehend

O Amazon Comprehend (prefixo do serviço: `comprehend`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Comprehend
- Tipos de recursos definidos pelo Amazon Comprehend
- Chaves de condição do Amazon Comprehend

Ações definidas pelo Amazon Comprehend

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchDetectDominantLanguage	Concede permissão para detectar o idioma ou os idiomas presentes na lista de documentos de texto	Read			
BatchDetectEntities	Concede permissão para detectar as entidades nomeadas ("pessoas", "lugares", "locais", etc.) em determinada lista de documentos de texto	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchDetectKeyPhrases	Concede permissão para detectar as frases na lista de documentos de texto que são mais indicativas do conteúdo	Read			
BatchDetectSentiment	Concede permissão para detectar o sentimento de um texto na lista de documentos (positivo, negativo, neutro ou misto)	Read			
BatchDetectSyntax	Concede permissão para detectar informações sintáticas (como parte da fala, tokens) em uma lista de documentos de texto	Leitura			
BatchDetectTargetedSentiment	Concede permissão para detectar sentimentos associados a entidades específicas (como marcas ou produtos) em determinada lista de documentos de texto	Leitura			
ClassifyDocument	Concede permissão para criar uma solicitação de classificação de documento para analisar um único documento em tempo real, usando um modelo personalizado previamente criado e treinado e um endpoint	Leitura	document-classifier-endpoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ContainsPiiEntities	Concede permissão para classificar as informações de identificação pessoal em determinados documentos em tempo real	Leitura			
CreateDataset	Concede permissão para criar um novo conjunto de dados em um flywheel	Gravar	flywheel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDocumentClassifier	Concede permissão para criar um classificador de documentos que pode ser usado usar para categorizar documentos	Write	document-classifier*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:ModelKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateEndpoint	Concede permissão para criar um endpoint específico do modelo para inferência síncrona de um modelo personalizado previamente treinado	Write	document-classifier*		
			document-classifier-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys	
			entity-recognizer*		
			entity-recognizer-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys	
			flywheel		
CreateEntityRecognizer	Concede permissão para criar um reconhecedor de entidade usando arquivos enviados	Gravar	entity-recognizer*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:ModelKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateFlywheel	Concede permissão para criar um novo flywheel que pode ser usado para treinar as versões de modelo	Gravar	flywheel*	aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:ModelKmsKey comprehend:DataLakeKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
			document-classifier		
			entity-recognizer		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteDocumentClassifier	Concede permissão para excluir um classificador de documentos criado anteriormente	Write	document-classifier*		
DeleteEndpoint	Concede permissão para excluir um endpoint específico do modelo para um modelo personalizado treinado anteriormente. Todos os endpoints devem ser excluídos para que o modelo seja excluído	Write	document-classifier-endpoint*		
			entity-recognizer-endpoint*		
DeleteEntityRecognizer	Concede permissão para excluir um reconhecedor de entidade enviado	Gravar	entity-recognizer*		
DeleteFlywheel	Concede permissão para excluir um flywheel	Gravar	flywheel*		
DeleteResourcePolicy	Concede permissão para remover a política do recurso	Gravar	document-classifier*		
			entity-recognizer*		
DescribeDataset	Concede permissão para obter as propriedades associadas a um conjunto de dados	Leitura	flywheel-dataset*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeDocumentClassificationJob	Concede permissão para obter as propriedades associadas a um trabalho de classificação de documento	Read	document-classification-job*		
DescribeDocumentClassifier	Concede permissão para obter as propriedades associadas a um classificador de documentos	Read	document-classifier*		
DescribeDominantLanguageDetectionJob	Concede permissão para obter as propriedades associadas a um trabalho de detecção de idioma dominante	Read	dominant-language-detection-job*		
DescribeEndpoint	Concede permissão para obter as propriedades associadas a um endpoint específico Use essa operação para obter o status de um endpoint	Read	document-classifier-endpoint* entity-recognizer-endpoint*		
DescribeEntitiesDetectionJob	Concede permissão para obter as propriedades associadas a um trabalho de detecção de entidades	Read	entities-detection-job*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeEntityRecognizer	Concede permissão para fornecer detalhes sobre um reconhecedor de entidades, incluindo status, buckets do S3 que contêm dados de treinamento, metadados do reconhecedor, métricas e assim por diante.	Read	entity-recognizer*		
DescribeEventsDetectionJob	Concede permissão para obter as propriedades associadas a um trabalho de detecção de eventos	Leitura	events-detection-job*		
DescribeFlywheel	Concede permissão para obter as propriedades associadas a um flywheel	Leitura	flywheel*		
DescribeFlywheelIteration	Concede permissão para obter as propriedades associadas a uma iteração de flywheel de um flywheel	Leitura	flywheel*		
				comprehend:FlywheelIterationId	
DescribeKeyPhrasesDetectionJob	Concede permissão para obter as propriedades associadas a um trabalho de detecção de frases-chave	Read	key-phrases-detection-job*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribePiiEntitiesDetectionJob	Concede permissão para obter as propriedades associadas a um trabalho de detecção de entidades de PII	Leitura	pii-entities-detection-job*		
DescribeResourcePolicy	Concede permissão para lera a política anexada ao recurso	Leitura	document-classifier*		
			entity-recognizer*		
DescribeSentimentDetectionJob	Concede permissão para obter as propriedades associadas a um trabalho de detecção de sentimentos	Leitura	sentiment-detection-job*		
DescribeTargetedSentimentDetectionJob	Concede permissão para obter as propriedades associadas a um trabalho de detecção de sentimentos direcionado	Leitura	targeted-sentiment-detection-job*		
DescribeTopicsDetectionJob	Concede permissão para obter as propriedades associadas a um trabalho de detecção de tópico	Read	topics-detection-job*		
DetectDominantLanguage	Concede permissão para detectar o idioma ou idiomas presentes no texto	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DetectEntities	Concede permissão para detectar as entidades nomeadas (“pessoas”, “lugares”, “locais”, etc.) no documento de texto fornecido	Read	entity-recognizer-endpoint		
DetectKeyPhrases	Concede permissão para detectar as frases no texto que são mais indicativas do conteúdo	Read			
DetectPiiEntities	Concede permissão para detectar as entidades de informação de identificação pessoal (“nome”, “SSN”, “PIN”, etc.) no documento de texto fornecido	Read			
DetectSentiment	Concede permissão para detectar o sentimento de um texto em um documento (positivo, negativo, neutro ou misto)	Read			
DetectSyntax	Concede permissão para detectar informações sintáticas (como parte da fala, tokens) em um documento de texto	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DetectTargetedSentiment	Concede permissão para detectar sentimentos associados a entidades específicas (como marcas ou produtos) em um documento	Leitura			
DetectToxicContent	Concede permissão para detectar conteúdo tóxico em uma determinada lista de segmentos de texto	Leitura			
ImportModel	Concede permissão para importar um modelo do Comprehend treinado	Gravar	document-classifier*		
			entity-recognizer*		
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:ModelKmsKey	
ListDatasets	Concede permissão para obter uma lista dos conjuntos de dados associados a um flywheel	Leitura	flywheel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDocumentClassificationJobs	Concede permissão para obter uma lista dos trabalhos de classificação de documentos enviados	Leitura			
ListDocumentClassifierSummaries	Concede permissão para obter uma lista de resumos dos classificadores de documentos criados	Leitura			
ListDocumentClassifiers	Concede permissão para obter uma lista dos classificadores de documentos criados	Leitura			
ListDominantLanguageDetectionJobs	Concede permissão para obter uma lista dos trabalhos de detecção de idioma dominante enviados	Leitura			
ListEndpoints	Concede permissão para obter uma lista de todos os endpoints existentes criados	Leitura			
ListEntitiesDetectionJobs	Concede permissão para obter uma lista dos trabalhos de detecção de entidade enviados	Leitura			
ListEntityRecognizerSummaries	Concede permissão para obter uma lista de resumos para os reconhecedores de entidade criados	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListEntityRecognizers	Concede permissão para obter uma lista das propriedades de todos os reconhecedores de entidades criados, incluindo os reconhecedores em treinamento no momento	Leitura			
ListEventsDetectionJobs	Concede permissão para obter uma lista de trabalhos de detecção de eventos enviados por você	Leitura			
ListFlywheelIterationHistory	Concede permissão para obter uma lista de iterações associadas de um flywheel	Leitura	flywheel*		
ListFlywheels	Concede permissão para obter uma lista dos flywheels criados	Leitura			
ListKeyPhrasesDetectionJobs	Concede permissão para obter uma lista dos trabalhos de detecção de frases-chave enviados	Leitura			
ListPiiEntitiesDetectionJobs	Concede permissão para obter uma lista de trabalhos de detecção de entidades de PII enviados	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListSentimentDetectionJobs	Concede permissão para obter uma lista de trabalhos de detecção de sentimentos enviados	Leitura			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	document-classification-job		
			document-classifier		
			document-classifier-endpoint		
			dominant-language-detection-job		
			entities-detection-job		
			entity-recognizer		
			entity-recognizer-endpoint		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			events-detection-job		
			flywheel		
			flywheel-dataset		
			key-phrases-detection-job		
			pii-entities-detection-job		
			sentiment-detection-job		
			targeted-sentiment-detection-job		
			topics-detection-job		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTargetedSentimentDetectionJobs	Concede permissão para obter uma lista de trabalhos de detecção de sentimentos direcionados que você enviou	Leitura			
ListTopicsDetectionJobs	Concede permissão para obter uma lista dos trabalhos de detecção de tópicos enviados	Leitura			
PutResourcePolicy	Concede permissão para anexar política ao recurso	Gravar	document-classifier*		
			entity-recognizer*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartDocumentClassificationJob	Concede permissão para iniciar um trabalho assíncrono de classificação de documentos	Write	document-classification-job*	aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
			document-classifier		
			flywheel		
StartDominantLanguageDetectionJob	Concede permissão para iniciar um trabalho assíncrono de detecção de idioma dominante para uma coleção de documentos	Write	dominant-language-detection-job*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartEntitiesDetectionJob	Concede permissão para iniciar um trabalho assíncrono de detecção de entidade para uma coleção de documentos	Write	entities-detection-job*	aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
			entity-recognizer		
			flywheel		
StartEventsDetectionJob	Concede permissão para iniciar um trabalho de detecção de eventos assíncrono para uma coleção de documentos	Gravar	events-detection-job*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:OutputKmsKey	
StartFlywheelIteration	Concede permissão para iniciar uma iteração de flywheel para um flywheel	Gravar	flywheel*		
StartKeyPhrasesDetectionJob	Concede permissão para iniciar um trabalho assíncrono de detecção de frases-chave para uma coleção de documentos	Write	key-phrases-detection-job*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
StartPiiEntitiesDetectionJob	Concede permissão para iniciar um trabalho assíncrono de detecção de entidades de PII para uma coleção de documentos	Write	pii-entities-detection-job*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:OutputKmsKey	
StartSentimentDetectionJob	Concede permissão para iniciar um trabalho assíncrono de detecção de sentimentos para uma coleção de documentos	Gravar	sentiment-detection-job*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
StartTargetedSentimentDetectionJob	Concede permissão para iniciar um trabalho assíncrono de detecção de sentimentos direcionado para uma coleção de documentos	Gravar	targeted-sentiment-detection-job*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
StartTopicsDetectionJob	Concede permissão para iniciar um trabalho assíncrono para detectar os tópicos mais comuns na coleção de documentos e as frases associadas a cada tópico	Write	topics-detection-job*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
StopDominantLanguageDetectionJob	Concede permissão para interromper um trabalho de detecção de idioma dominante	Write	dominant-language-detection-job*		
StopEntitiesDetectionJob	Concede permissão para interromper um trabalho de detecção de entidade	Write	entities-detection-job*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopEventsDetectionJob	Concede permissão para interromper um trabalho de detecção de eventos	Write	events-detection-job*		
StopKeyPhrasesDetectionJob	Concede permissão para interromper um trabalho de detecção de frases-chave	Write	key-phrases-detection-job*		
StopPiiEntitiesDetectionJob	Concede permissão para interromper um trabalho de detecção de entidades de PII	Write	pii-entities-detection-job*		
StopSentimentDetectionJob	Concede permissão para interromper um trabalho de detecção de sentimentos	Gravar	sentiment-detection-job*		
StopTargetedSentimentDetectionJob	Concede permissão para interromper um trabalho de detecção de sentimentos direcionado	Gravar	targeted-sentiment-detection-job*		
StopTrainingDocumentClassifier	Concede permissão para interromper um trabalho de treinamento de classificador de documentos criado anteriormente	Write	document-classifier*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopTrainingEntityRecognizer	Concede permissão para interromper um trabalho de treinamento de reconhecimento de entidade criado anteriormente	Write	entity-recognizer*		
TagResource	Concede permissão para marcar um recurso com determinados pares de chave-valor	Marcação	document-classification-job		
			document-classifier		
			document-classifier-endpoint		
			dominant-language-detection-job		
			entities-detection-job		
			entity-recognizer		
			entity-recognizer-endpoint		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			events-detection-job		
			flywheel		
			flywheel-dataset		
			key-phrases-detection-job		
			pii-entities-detection-job		
			sentiment-detection-job		
			targeted-sentiment-detection-job		
			topics-detection-job		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso com determinada chave	Marcação	document-classification-job		
			document-classifier		
			document-classifier-endpoint		
			dominant-language-detection-job		
			entities-detection-job		
			entity-recognizer		
			entity-recognizer-endpoint		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			events-detection-job		
			flywheel		
			flywheel-dataset		
			key-phrases-detection-job		
			pii-entities-detection-job		
			sentiment-detection-job		
			targeted-sentiment-detection-job		
			topics-detection-job		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateEndpoint	Concede permissão para atualizar informações sobre o endpoint especificado	Gravar	document-classifier-endpoint*		
			entity-recognizer-endpoint*		
			flywheel		
UpdateFlywheel	Concede permissão para atualizar a configuração de um flywheel	Gravar	flywheel*	comprehend:VolumeKmsKey comprehend:ModelKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
			document-classifier		
			entity-recognizer		

Tipos de recursos definidos pelo Amazon Comprehend

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Tipos de recursos	ARN	Chaves de condição
entities-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:entities-detection-job/${JobId}	aws:ResourceTag/${TagKey}
pii-entities-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:pii-entities-detection-job/${JobId}	aws:ResourceTag/${TagKey}
events-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:events-detection-job/${JobId}	aws:ResourceTag/${TagKey}
key-phrases-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:key-phrases-detection-job/${JobId}	aws:ResourceTag/${TagKey}
sentiment-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:sentiment-detection-job/${JobId}	aws:ResourceTag/${TagKey}
topics-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:topics-detection-job/${JobId}	aws:ResourceTag/${TagKey}
document-classification-job	arn:${Partition}:comprehend:${Region}:${Account}:document-classification-job/${JobId}	aws:ResourceTag/${TagKey}
flywheel	arn:${Partition}:comprehend:${Region}:${Account}:flywheel/${FlywheelName}	aws:ResourceTag/${TagKey}
flywheel-dataset	arn:${Partition}:comprehend:${Region}:${Account}:flywheel/${FlywheelName}/dataset/${DatasetName}	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Comprehend

O Amazon Comprehend define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso exigindo valores de etiquetas presentes em uma solicitação de criação de recurso	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelo valor de etiqueta necessário associado ao recurso	String
aws:TagKeys	Filtra o acesso exigindo a presença de etiquetas obrigatórias na solicitação	ArrayOfString
comprehend:DataLakeKmsKey	Filtra o acesso pela chave DataLake Kms associada ao recurso flywheel na solicitação	ARN
comprehend:FlywheelIterationId	Filtra o acesso por ID de iteração específico para um flywheel	String
comprehend:ModelKmsKey	Filtra o acesso pela chave KMS de modelo associada ao recurso na solicitação	ARN
comprehend:OutputKmsKey	Filtra o acesso pela chave KMS de saída associada ao recurso na solicitação	ARN

Chaves de condição	Descrição	Tipo
comprehend:VolumeKmsKey	Filtra o acesso pela chave do KMS de volume associada ao recurso na solicitação	ARN
comprehend:VpcSecurityGroupIds	Filtra o acesso pela lista de todos os IDs de grupo de segurança da VPC associados ao recurso na solicitação	ArrayOfString
comprehend:VpcSubnets	Filtra o acesso pela lista de todas as sub-redes da VPC associadas ao recurso na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Comprehend Medical

O Amazon Comprehend Medical (prefixo de serviço: `comprehendmedical`) fornece os recursos, ações e chaves de contexto de condição específicos do serviço a seguir para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Comprehend Medical
- Tipos de recursos definidos pelo Amazon Comprehend Medical
- Chaves de condição do Amazon Comprehend Medical

Ações definidas pelo Amazon Comprehend Medical

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou

ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeEntitiesDetectionV2Job	Concede permissão para descrever as propriedades de um trabalho de detecção da entidade médica que você enviou	Read			
DescribeICD10CMInferenceJob	Concede permissão para descrever as propriedades de um trabalho de vinculação ICD-10-CM que você enviou	Read			
DescribePHIDetectionJob	Concede permissão para descrever as propriedades de um trabalho de detecção da entidade PHI que você enviou	Leitura			
DescribeRxNormInferenceJob	Concede permissão para descrever as propriedades de um trabalho RxNorm vinculado que você enviou	Leitura			
DescribeSNOMEDCTInferenceJob	Concede permissão para descrever as propriedades de um trabalho de vinculação SNOMED-CT que você enviou	Leitura			
DetectEntitiesV2	Concede permissão para detectar as entidades médicas nomeadas e suas relações e características no documento de texto fornecido	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DetectPHI	Concede permissão para detectar as entidades de informações de saúde protegidas (PHI) no documento de texto fornecido	Read			
InferICD10CM	Concede permissão para detectar as entidades de condição médica no documento de texto fornecido e vinculá-las aos códigos ICD-10-CM	Leitura			
InferRxNorm	Concede permissão para detectar as entidades medicamentosas no documento de texto fornecido e vinculá-las aos identificadores conceituais RxCUI do banco de dados da National Library of Medicine RxNorm	Leitura			
InferSNOMEDCT	Concede permissão para detectar a condição médica, a anatomia e as entidades de teste, tratamento e procedimento no documento de texto fornecido e vinculá-las aos códigos SNOMED-CT	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListEntitiesDetectionV2Jobs	Concede permissão para obter uma lista dos trabalhos de detecção da entidade médica que você enviou	Read			
ListICD10CMInferenceJobs	Concede permissão para listar os trabalhos de vinculação ICD-10-CM que você enviou	Read			
ListPHIDetectionJobs	Concede permissão para listar os trabalhos de detecção de entidade PHI que você enviou	Leitura			
ListRxNormInferenceJobs	Concede permissão para listar os trabalhos RxNorm vinculados que você enviou	Leitura			
ListSNOMEDCTInferenceJobs	Concede permissão para listar os trabalhos de vinculação SNOMED-CT que você enviou	Leitura			
StartEntitiesDetectionV2Job	Concede permissão para iniciar um trabalho médico assíncrono de detecção da entidade para uma coleção de documentos	Write			
StartICD10CMInferenceJob	Concede permissão para iniciar um trabalho de vinculação ICD-10-CM assíncrono para uma coleção de documentos	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartPHIDetectionJob	Concede permissão para iniciar um trabalho assíncrono de detecção de entidade PHI para uma coleção de documentos	Gravar			
StartRxNormInferenceJob	Concede permissão para iniciar um trabalho de RxNorm vinculação assíncrona para uma coleção de documentos	Gravar			
StartSNOMEDCTInferenceJob	Concede permissão para iniciar um trabalho de vinculação SNOMED-CT assíncrono para uma coleção de documentos	Gravar			
StopEntitiesDetectionV2Job	Concede permissão para interromper um trabalho de detecção da entidade médica	Write			
StopICD10CMInferenceJob	Concede permissão para interromper um trabalho de vinculação ICD-10-CM	Write			
StopPHIDetectionJob	Concede permissão para interromper um trabalho de detecção da entidade PHI	Gravar			
StopRxNormInferenceJob	Concede permissão para interromper uma tarefa RxNorm vinculada	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopSNOMEDCTInferenceJob	Concede permissão para interromper um trabalho de vinculação SNOMED-CT	Gravar			

Tipos de recursos definidos pelo Amazon Comprehend Medical

O Amazon Comprehend Medical não oferece suporte à especificação do ARN de um recurso no elemento `Resource` de uma declaração de política do IAM. Para conceder acesso ao Amazon Comprehend Medical, especifique `"Resource": "*"` na política.

Chaves de condição do Amazon Comprehend Medical

O Amazon Comprehend Medical define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Compute Optimizer

AWS O Compute Optimizer (prefixo do serviço`compute-optimizer`:) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Compute Optimizer
- Tipos de recursos definidos pelo AWS Compute Optimizer
- Chaves de condição do AWS Compute Optimizer

Ações definidas pelo AWS Compute Optimizer

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteRecommendationPreferences	Concede permissão para excluir as preferências de recomendação	Gravar		compute-optimizer:ResourceType	autoscaling:DescribeAutoScalingGroups ec2:DescribeInstances rds:DescribeDBClusters rds:DescribeDBInstances

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeRecommendationExportJobs	Concede permissão para exibir o status dos trabalhos de exportação de recomendação	Lista			
ExportAutoScalingGroupRecommendations	Concede permissão para exportar recomendações de AutoScaling grupos para o S3 para as contas fornecidas	Gravar			autoscaling:DescribeAutoScalingGroups compute-optimizer:GetAutoScalingGroupRecommendations
ExportEBSVolumeRecommendations	Concede permissão para exportar recomendações de volumes do EBS para o S3 para as contas fornecidas	Gravar			compute-optimizer:GetEBSVolumeRecommendations ec2:DescribeVolumes

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ExportEC2InstanceRecommendations	Concede permissão para exportar recomendações de EC2 instâncias para o S3 para as contas fornecidas	Gravar			compute-optimizer:GetEC2InstanceRecommendations ec2:DescribeInstances
ExportECSServiceRecommendations	Concede permissão para exportar recomendações de serviço do ECS para o S3 para as contas fornecidas	Gravar			compute-optimizer:GetECSServiceRecommendations ecs:ListClusters ecs:ListServices
ExportIdleRecommendations	Concede permissão para exportar recomendações inativas para o S3 para as contas fornecidas	Gravar			compute-optimizer:GetIdleRecommendations

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ExportLambdaFunctionRecommendations	Concede permissão para exportar recomendações de funções do Lambda para o S3 para as contas fornecidas	Gravar			compute-optimizer:GetLambdaFunctionRecommendations lambda:ListFunctions lambda:ListProvisionedConcurrencyConfigs
ExportLicenseRecommendations	Concede permissão para exportar recomendações de licenças para o S3 para as contas fornecidas	Gravar			compute-optimizer:GetLicenseRecommendations ec2:DescribeInstances

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ExportRDSDatabaseRecommendations	Concede permissão para exportar recomendações do RDS para o S3 nas contas fornecidas	Gravar			compute-optimizer:GetRDSDatabaseRecommendations rds:DescribeDBClusters rds:DescribeDBInstances
GetAutoScalingGroupRecommendations	Concede permissão para obter recomendações para os AutoScaling grupos fornecidos	Lista			autoscaling:DescribeAutoScalingGroups
GetEBSVolumeRecommendations	Concede permissão para obter recomendações para os volumes EBS fornecidos	Lista			ec2:DescribeVolumes
GetEC2InstanceRecommendations	Concede permissão para obter recomendações para as EC2 instâncias fornecidas	Lista			ec2:DescribeInstances
GetEC2RecommendationProjectedMetrics	Concede permissão a fim de obter as métricas projetadas de recomendação da instância especificada.	Lista			ec2:DescribeInstances

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetECSServiceRecommendationProjectedMetrics	Concede permissão para obter as métricas projetadas de recomendação do serviço do ECS especificado	Lista			
GetECSServiceRecommendations	Concede permissão para obter recomendações para os serviços do ECS fornecidos	Lista			ecs:ListClusters ecs:ListServices

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetEffectiveRecommendationPreferences	Concede permissão para obter preferências de recomendação que estão em vigor	Leitura		compute-optimizer:ResourceType	autoscaling:DescribeAutoScalingGroups autoscaling:DescribeAutoScalingInstances ec2:DescribeInstances rds:DescribeDBClusters rds:DescribeDBInstances
GetEnrollmentStatus	Concede permissão a fim de obter o status de inscrição para a conta especificada.	Lista			
GetEnrollmentStatusesForOrganization	Concede permissão para obter o status de inscrição das contas-membro da organização	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetIdleRecommendations	Concede permissão para obter recomendações de inatividade para a (s) conta (s) especificada (s)	Lista			
GetLambdaFunctionRecommendations	Concede permissão para obter recomendações para as funções Lambda fornecidas	Lista			lambda:ListFunctions lambda:ListProvisionedConcurrencyConfigs
GetLicenseRecommendations	Concede permissão para obter recomendações de licenças para as contas especificadas	Lista			ec2:DescribeInstances
GetRDSDatabaseRecommendationProjectedMetrics	Concede permissão a fim de obter as métricas projetadas de recomendação da instância especificada.	Lista			rds:DescribeDBClusters rds:DescribeDBInstances

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetRDSDatabaseRecommendations	Concede permissão para obter recomendações do RDS para as contas especificadas	Lista			rds:DescribeDBClusters rds:DescribeDBInstances
GetRecommendationPreferences	Concede permissão para obter preferências de recomendações	Leitura		compute-optimizer:ResourceType	
GetRecommendationSummaries	Concede permissão a fim de obter os resumos de recomendação para a(s) conta(s) especificada(s).	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutRecommendationPreferences	Concede permissão para colocar as preferências de recomendação	Gravar		compute-optimizer:ResourceType	autoscaling:DescribeAutoScalingGroups autoscaling:DescribeAutoScalingInstances ec2:DescribeInstances rds:DescribeDBClusters rds:DescribeDBInstances
UpdateEnrollmentStatus	Concede permissão para atualizar o status de inscrição.	Write			

Tipos de recursos definidos pelo AWS Compute Optimizer

AWS O Compute Optimizer não suporta a especificação de um ARN de recurso `Resource` no elemento de uma declaração de política do IAM. Para conceder acesso ao AWS Compute Optimizer, especifique `"Resource": "*"` na política.

Chaves de condição do AWS Compute Optimizer

AWS O Compute Optimizer define as seguintes chaves de condição que podem ser usadas no elemento de uma `Condition` política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
compute-optimizer:ResourceType	Filtra o acesso pelo tipo de recurso	String

Ações, recursos e chaves de condição do AWS Config

AWS Config (prefixo do serviço:`config`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Config
- Tipos de recursos definidos pelo AWS Config
- Chaves de condição do AWS Config

Ações definidas pelo AWS Config

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateResourceTypes	Concede permissão para adicionar todos os tipos de recursos especificados ao gravador RecordingGroup de configuração e inclui esses tipos de recursos ao gravar	Gravar	ConfigurationRecorder*		
BatchGetAggregateResourceConfig	Concede permissão para retornar os itens de configuração atuais dos recursos que estão presentes em seu agregador AWS Config	Leitura	ConfigurationAggregator*		
BatchGetResourceConfig	Concede permissão para retornar a configuração atual para um ou mais recursos solicitados	Read			
DeleteAggregationAuthorization	Concede permissão para excluir a autorização concedida à conta agregadora de configuração especificada em uma região especificada	Gravar	AggregationAuthorization*		
DeleteConfigRule	Concede permissão para excluir a regra AWS Config especificada e todos os seus resultados de avaliação	Gravar	ConfigRule*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteConfigurationAggregator	Concede permissão para excluir o agregador de configuração especificado e os dados agregados associados ao agregador	Gravar	ConfigurationAggregator*		
DeleteConfigurationRecorder	Concede permissão para excluir o gravador de configuração gerenciado pelo cliente	Gravar	ConfigurationRecorder*		
DeleteConformancePack	Concede permissão para excluir o pacote de conformidade especificado e todas as regras de AWS Config e todos os resultados de avaliação dentro desse pacote de conformidade	Gravar	ConformancePack*		
DeleteDeliveryChannel	Concede permissão para excluir o canal de entrega	Write			
DeleteEvaluationResults	Concede permissão para excluir os resultados da avaliação para a regra de configuração especificada	Write	ConfigRule*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteOrganizationConfigRule	Concede permissão para excluir a regra de configuração da organização especificada e todos os resultados de avaliação de todas as contas de membros dessa organização	Write	OrganizationConfigRule*		
DeleteOrganizationConformancePack	Concede permissão para excluir o pacote de conformidade da organização especificado e todos os resultados de avaliação de todas as contas de membros dessa organização	Write	OrganizationConformancePack*		
DeletePendingAggregationRequest	Concede permissão para excluir solicitações de autorização pendentes para uma conta agregadora especificada em uma região especificada	Write			
DeleteRemediationConfiguration	Concede permissão para excluir a configuração de correção	Gravar	RemediationConfiguration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteRemediationExceptions	Concede permissão para excluir uma ou mais exceções de remediação para chaves de recursos específicas para uma regra de configuração AWS específica	Gravar			
DeleteResourceConfig	Concede permissão para registrar o estado de configuração de um recurso personalizado excluído	Write			
DeleteRetentionConfiguration	Concede permissão para excluir a configuração de retenção	Gravar			
DeleteServiceLinkedConfigurationRecorder	Concede permissão para excluir o gravador de configuração vinculado ao serviço	Gravar	ConfigurationRecorder*		
				config:ConfigurationRecorderServicePrincipal	
DeleteStoredQuery	Concede permissão para excluir a consulta armazenada para um Conta da AWS em um Região da AWS	Gravar	StoredQuery*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeliverConfigSnapshot	Concede permissão para agendar a entrega de um snapshot de configuração para o bucket do Amazon S3 no canal de entrega especificado	Read			
DescribeAggregateComplianceByConfigRules	Concede permissão para devolver uma lista de regras compatíveis e não conformes com o número de recursos para regras compatíveis e não conformes	Read	ConfigurationAggregator*		
DescribeAggregateComplianceByConformancePacks	Concede permissão para devolver uma lista de pacotes de compatibilidade compatíveis e não compatíveis, juntamente com a contagem de regras compatíveis, não compatíveis e totais dentro de cada pacote de compatibilidade	Read	ConfigurationAggregator*		
DescribeAggregationAuthorizations	Concede permissão para devolver uma lista de autorizações concedidas a várias contas agregadoras e regiões	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeCompliance ByConfigRule	Concede permissão para indicar se as regras de AWS Config especificadas estão em conformidade	Leitura			
DescribeCompliance ByResource	Concede permissão para indicar se os AWS recursos especificados estão em conformidade	Leitura			
DescribeConfigRule EvaluationStatus	Concede permissão para retornar informações de status para cada uma de suas regras de Config AWS gerenciadas	Leitura			
DescribeConfigRules	Concede permissão para retornar detalhes sobre suas regras de AWS Config	Lista			
DescribeConfigurationAggregatorSourcesStatus	Concede permissão para devolver informações de status para fontes dentro de um agregador	Read	ConfigurationAggregator*		
DescribeConfigurationAggregators	Concede permissão para devolver os detalhes de um ou mais agregadores de configuração	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeConfigurationRecorderStatus	Concede permissão para devolver o status atual do gravador de configuração especificado	Read	ConfigurationRecorder*		
				config:ConfigurationRecorderServicePrincipal	
DescribeConfigurationRecorders	Concede permissão para devolver os nomes de um ou mais gravadores de configuração especificados	Leitura	ConfigurationRecorder*		
				config:ConfigurationRecorderServicePrincipal	
DescribeConformancePackCompliance	Concede permissão para devolver informações de conformidade para cada regra nesse pacote de conformidade	Read	ConformancePack*		
DescribeConformancePackStatus	Concede permissão para fornecer um ou mais status de implantação de pacotes de conformidade	Read			
DescribeConformancePacks	Concede permissão para retornar uma lista de um ou mais pacotes de conformidade	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeDeliveryChannelStatus	Concede permissão para retornar o status atual do canal de entrega especificado	Read			
DescribeDeliveryChannels	Concede permissão para devolver detalhes sobre o canal de entrega especificado	List			
DescribeOrganizationConfigRuleStatuses	Concede permissão para fornecer status de implantação da regra de configuração da organização para uma organização	Read			
DescribeOrganizationConfigRules	Concede permissão para devolver uma lista de regras de configuração da organização	List			
DescribeOrganizationConformancePackStatuses	Concede permissão para fornecer status de implantação do pacote de conformidade da organização para uma organização	Read			
DescribeOrganizationConformancePacks	Concede permissão para devolver uma lista de pacotes de conformidade da organização	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribePendingAggregationRequests	Concede permissão para devolver uma lista de todas as solicitações de agregação pendentes	List			
DescribeRemediationConfigurations	Concede permissão para devolver os detalhes de uma ou mais configurações de correção	List	RemediationConfiguration*		
DescribeRemediationExceptions	Concede permissão para devolver os detalhes de uma ou mais exceções de correção	List			
DescribeRemediationExecutionStatus	Concede permissão para fornecer uma visualização detalhada de uma execução de remediação para um conjunto de recursos, incluindo estado, carimbos de data/hora e quaisquer mensagens de erro para etapas que falharam	Read	RemediationConfiguration*		
DescribeRetentionConfigurations	Concede permissão para devolver os detalhes de uma ou mais configurações de retenção	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateResourceTypes	Concede permissão para remover todos os tipos de recursos especificados do gravador RecordingGroup de configuração e exclui esses tipos de recursos durante a gravação	Gravar	ConfigurationRecorder*		
GetAggregateComplianceDetailsByConfigRule	Concede permissão para retornar os resultados da avaliação da regra AWS Config especificada para um recurso específico em uma regra	Leitura	ConfigurationAggregator*		
GetAggregateConfigRuleComplianceSummary	Concede permissão para devolver o número de regras compatíveis e não conformes para uma ou mais contas e regiões em um agregador	Read	ConfigurationAggregator*		
GetAggregateConformancePackComplianceSummary	Concede permissão para devolver o número de pacotes de compatibilidade compatíveis e não compatíveis para uma ou mais contas e regiões em um agregador	Leitura	ConfigurationAggregator*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAggregateDiscoveredResourceCounts	Concede permissão para retornar as contagens de recursos em todas as contas e regiões que estão presentes em seu AWS agregador Config	Leitura	ConfigurationAggregator*		
GetAggregateResourceConfig	Concede permissão para devolver o item de configuração que é agregado para seu recurso específico em uma conta e região de origem específicas	Leitura	ConfigurationAggregator*		
GetComplianceDetailsByConfigRule	Concede permissão para retornar os resultados da avaliação para a regra AWS Config especificada	Leitura	ConfigRule*		
GetComplianceDetailsByResource	Concede permissão para retornar os resultados da avaliação para o AWS recurso especificado	Leitura			
GetComplianceSummaryByConfigRule	Concede permissão para retornar o número de regras do AWS Config compatíveis e não compatíveis, até um máximo de 25 para cada	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetComplianceSummaryByResourceType	Concede permissão para devolver o número de recursos que estão em conformidade e o número que não estão em conformidade	Leitura			
GetConformancePackComplianceDetails	Concede permissão para devolver detalhes de conformidade de um pacote de conformidade para todos os AWS recursos monitorados pelo pacote de conformidade	Leitura	ConformancePack*		
GetConformancePackComplianceSummary	Concede permissão para fornecer resumo de conformidade para um ou mais pacotes de conformidade	Leitura	ConformancePack*		
GetCustomRulePolicy	Concede permissão para retornar a definição da política contendo a lógica da sua regra AWS Config Custom Policy	Leitura	ConfigRule*		
GetDiscoveredResourceCounts	Concede permissão para retornar os tipos de recursos, o número de cada tipo de recurso e o número total de recursos que o AWS Config está registrando nessa região para seu Conta da AWS	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetOrganizationConfigRuleDetailedStatus	Concede permissão para devolver status detalhado para cada conta de membro dentro de uma organização para uma determinada regra de configuração da organização	Read	OrganizationConfigRule*		
GetOrganizationConformancePackDetailedStatus	Concede permissão para retornar status detalhado para cada conta de membro dentro de uma organização para um determinado pacote de conformidade da organização	Leitura	OrganizationConformancePack*		
GetOrganizationCustomRulePolicy	Concede permissão para retornar a definição de política contendo a lógica da regra AWS Config Custom Policy da sua organização	Leitura	OrganizationConfigRule*		
GetResourceConfigHistory	Concede permissão para devolver uma lista de itens de configuração para o recurso especificado	Leitura			
GetResourceEvaluationSummary	Concede permissão para retornar o resumo das avaliações do recurso para um ID específico de avaliação de recurso	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetStoredQuery	Concede permissão para devolver os detalhes de uma consulta armazenada específica	Read	StoredQuery*		
ListAggregateDiscoveredResources	Concede permissão para aceitar um tipo de recurso e devolve uma lista de identificadores de recursos agregados para um tipo de recurso específico entre contas e regiões	Lista	ConfigurationAggregator*		
ListConfigurationRecorders	Concede permissão para listar os resumos do gravador de configuração para um em um Conta da AWS Região da AWS	Lista			
ListConformancePackComplianceScores	Concede permissão para retornar a porcentagem de combinações de recursos e regras compatíveis em um pacote de conformidade em comparação com o número total de combinações possíveis de regras e recursos	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDiscoveredResources	Concede permissão para aceitar um tipo de recurso e devolve uma lista de identificadores de recursos para os recursos desse tipo	Lista			
ListResourceEvaluations	Concede permissão para listar os resumos de avaliação de recursos de um Conta da AWS em um Região da AWS	Lista			
ListStoredQueries	Concede permissão para listar as consultas armazenadas para um Conta da AWS em um Região da AWS	Lista			
ListTagsForResource	Concede permissão para listar as tags do AWS recurso Config	Leitura	AggregationAuthorization		
			ConfigRule		
			ConfigurationAggregator		
			ConfigurationRecorder		
			ConformancePack		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			OrganizationConfigRule		
			OrganizationConformancePack		
			StoredQuery		
PutAggregationAuthorization	Concede permissão para autorizar a conta e a região agregadora a coletar dados da conta e região de origem	Gravar	AggregationAuthorization*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutConfigRule	Concede permissão para adicionar ou atualizar uma regra AWS Config para avaliar se seus AWS recursos estão em conformidade com as configurações desejadas	Gravar	ConfigRule*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutConfigurationAggregator	Concede permissão para criar e atualizar o agregador de configuração com as contas e regiões de origem selecionadas	Gravar	ConfigurationAggregator*		iam:PassRole organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators
				aws:RequestTag/${TagKey} aws:TagKeys	
PutConfigurationRecorder	Concede permissão para criar ou atualizar um gravador de configuração gerenciado pelo cliente para registrar as configurações de recursos selecionadas	Gravar	ConfigurationRecorder*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutConformancePack	Concede permissão para criar ou atualizar um pacote de conformidade	Write	ConformancePack*		iam:CreateServiceLinkedRole iam:PassRole s3:GetObject s3:ListBucket ssm:GetDocument
PutDeliveryChannel	Concede permissão para criar um objeto de canal de entrega para fornecer informações de configuração a um bucket do Amazon S3 e tópico do Amazon SNS	Gravar			
PutEvaluations	Concede permissão para ser usado por uma função AWS Lambda para fornecer resultados de avaliação ao Config AWS	Gravar			
PutExternalEvaluation	Concede permissão para entregar o resultado da avaliação ao AWS Config	Gravar	ConfigRule*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutOrganizationConfigRule	Concede permissão para adicionar ou atualizar a regra de configuração da organização para toda a organização, avaliando se seus AWS recursos estão em conformidade com as configurações desejadas	Gravar	OrganizationConfigRule*		iam:CreateServiceLinkedRole iam:PassRole organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutOrganizationConformancePack	Concede permissão para adicionar ou atualizar o pacote de conformidade organizacional para toda a organização, avaliando se seus AWS recursos estão em conformidade com as configurações desejadas	Gravar	OrganizationConformancePack*		iam:CreateServiceLinkedRole iam:PassRole organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators s3:GetObject
PutRemediationConfigurations	Concede permissão para adicionar ou atualizar a configuração de remediação com uma regra AWS Config específica com o alvo ou a ação selecionada	Gravar	RemediationConfiguration*		iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutRemediationExceptions	Concede permissão para adicionar ou atualizar exceções de remediação para recursos específicos para uma regra de Config AWS específica	Gravar			
PutResourceConfig	Concede permissão para registrar o estado de configuração do recurso fornecido na solicitação	Gravar			
PutRetentionConfiguration	Concede permissão para criar e atualizar a configuração de retenção com detalhes sobre o período de retenção (número de dias) em que o AWS Config armazena suas informações históricas	Gravar			
PutServiceLinkedConfigurationRecorder	Concede permissão para criar um novo gravador de configuração vinculado ao serviço para registrar as configurações de recursos no escopo do serviço vinculado	Gravar		aws:RequestTag/${TagKey} aws:TagKeys config:ConfigurationRecorderServicePrincipal	iam:CreateServiceLinkedRole iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutStoredQuery	Concede permissão para salvar uma nova consulta ou atualiza uma consulta salva existente	Gravar	StoredQuery*		
				aws:RequestTag/${TagKey} aws:TagKeys	
SelectAggregateResourceConfig	Concede permissão para aceitar um comando SELECT da linguagem de consulta estruturada (SQL) e um agregador para consultar o estado de configuração dos AWS recursos em várias contas e regiões, realizar a pesquisa correspondente e retornar configurações de recursos que correspondam às propriedades	Leitura	ConfigurationAggregator*		
SelectResourceConfig	Concede permissão para aceitar um comando SELECT de linguagem de consulta estruturada (SQL), executa a pesquisa correspondente e retorna configurações de recursos correspondentes às propriedades	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartConfigRulesEvaluation	Concede permissão para avaliar seus recursos em relação às regras de configuração especificadas	Gravar	ConfigRule*		
StartConfigurationRecorder	Concede permissão ao gravador de configuração gerenciado pelo cliente para começar a gravar as configurações dos AWS recursos que você selecionou para gravar em seu Conta da AWS	Gravar	ConfigurationRecorder*		
StartRemediationExecution	Concede permissão para executar uma remediação sob demanda para as regras de AWS Config especificadas em relação à última configuração de remediação conhecida	Gravar			iam:PassRole
StartResourceEvaluation	Concede permissão para avaliar os detalhes do seu recurso em relação às regras de AWS Config em sua conta	Gravar			cloudformation:DescribeType

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopConfigurationRecorder	Concede permissão ao gravador de configuração gerenciado pelo cliente para interromper o registro das configurações dos AWS recursos que você selecionou para gravar em seu Conta da AWS	Gravar	ConfigurationRecorder*		
TagResource	Concede permissão para associar as etiquetas especificadas a um recurso com o resourceArn especificado	Marcação	AggregationAuthorization		
			ConfigRule		
			ConfigurationAggregator		
			ConfigurationRecorder		
			ConformancePack		
			OrganizationConfigRule		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			OrganizationConformancePack		
			StoredQuery		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para excluir etiquetas especificadas de um recurso	Marcação	AggregationAuthorization		
			ConfigRule		
			ConfigurationAggregator		
			ConfigurationRecorder		
			ConformancePack		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			OrganizationConfigRule		
			OrganizationConformancePack		
			StoredQuery		
				aws:TagKeys	

Tipos de recursos definidos pelo AWS Config

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
AggregationAuthorization	`arn:${Partition}:config:${Region}:${Account}:aggregation-authorization/${AggregatorAccount}/${AggregatorRegion}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
ConfigurationAggregator	arn:${Partition}:config:${Region}:${Account}:config-aggregator/${AggregatorId}	aws:ResourceTag/${TagKey}
ConfigRule	arn:${Partition}:config:${Region}:${Account}:config-rule/${ConfigRuleId}	aws:ResourceTag/${TagKey}
ConformancePack	arn:${Partition}:config:${Region}:${Account}:conformance-pack/${ConformancePackName}/${ConformancePackId}	aws:ResourceTag/${TagKey}
OrganizationConfigRule	arn:${Partition}:config:${Region}:${Account}:organization-config-rule/${OrganizationConfigRuleId}	aws:ResourceTag/${TagKey}
OrganizationConformancePack	arn:${Partition}:config:${Region}:${Account}:organization-conformance-pack/${OrganizationConformancePackId}	aws:ResourceTag/${TagKey}
RemediationConfiguration	arn:${Partition}:config:${Region}:${Account}:remediation-configuration/${RemediationConfigurationId}	
StoredQuery	arn:${Partition}:config:${Region}:${Account}:stored-query/${StoredQueryName}/${StoredQueryId}	aws:ResourceTag/${TagKey}
ConfigurationRecorder	arn:${Partition}:config:${Region}:${Account}:configuration-recorder/${RecorderName}/${RecorderId}	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Config

AWS Config define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições

sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelo conjunto de valores permitido para cada uma das etiquetas	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelo valor-etiqueta associado ao recurso	String
aws:TagKeys	Filtra o acesso pela presença de etiquetas obrigatórias na solicitação	ArrayOfString
config:ConfigurationRecorderServicePrincipal	Filtra o acesso pelo principal de serviço do gravador de configuração	String

Ações, recursos e chaves de condição do Amazon Connect Cases

O Amazon Connect Cases (prefixo do serviço: `cases`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Connect Cases

- Tipos de recursos definidos pelo Amazon Connect Cases
- Chaves de condição do Amazon Connect Cases

Ações definidas pelo Amazon Connect Cases

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchGetCaseRule	Concede permissão para recuperar informações sobre as regras do caso no domínio do caso	Leitura	CaseRule*		
			Domain*		
BatchGetField	Concede permissão para recuperar informações sobre os campos no domínio do caso	Leitura	Domain*		
			Field*		
BatchPutFieldOptions	Concede permissão para atualizar as opções de campo no domínio do caso	Gravar	Domain*		
			Field*		
CreateCase	Concede permissão para criar um caso no domínio do caso	Gravar	Case*		
			Domain*		
			Field*		
			Template*		
				connect:UserArn	
CreateCaseRule	Concede permissão para criar uma regra de caso no domínio do caso	Gravar	CaseRule*		
			Domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDomain	Concede permissão para criar um novo domínio de caso	Gravar			
CreateField	Concede permissão para criar um campo no domínio do caso	Gravar	Domain*		
			Field*		
CreateLayout	Concede permissão para criar um layout no domínio do caso	Gravar	Domain*		
			Layout*		
CreateRelatedItem	Concede permissão para criar um item associado a um caso no domínio do caso	Gravar	Case*		
			Domain*		
			RelatedItem*		
				connect:UserArn	
CreateTemplate	Concede permissão para criar um modelo no domínio do caso	Gravar	Domain*		
			Layout*		
			Template*		
DeleteCase	Concede permissão para excluir o caso no domínio do caso	Gravar	Case*		
			Domain*		
DeleteCaseRule	Concede permissão para excluir a regra do caso no domínio do caso	Gravar	CaseRule*		
			Domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteDomain	Concede permissão para excluir o domínio	Gravar	Domain*		
DeleteField	Concede permissão para excluir o campo no domínio do caso	Gravar	Domain*		
			Field*		
DeleteLayout	Concede permissão para excluir o layout no domínio do caso	Gravar	Domain*		
			Layout*		
DeleteRelatedItem	Concede permissão para excluir o item relacionado associado ao caso no domínio do caso	Gravar	Case*		
			Domain*		
			RelatedItem*		
DeleteTemplate	Concede permissão para excluir o modelo no domínio do caso	Gravar	Domain*		
			Template*		
GetCase	Concede permissão para recuperar informações sobre um caso no domínio do caso	Leitura	Case*		
			Domain*		
			Field*		
GetCaseAuditEvents	Concede permissão para exibir o histórico de auditoria de um caso	Leitura	Case*		
			Domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetCaseEventConfiguration	Concede permissão para recuperar informações sobre a configuração de evento do caso no domínio do caso	Leitura	Domain*		
GetDomain	Concede permissão para recuperar informações sobre o domínio do caso	Leitura	Domain*		
GetLayout	Concede permissão para recuperar informações sobre o layout no domínio do caso	Leitura	Domain*		
			Layout*		
GetTemplate	Concede permissão para recuperar informações sobre o modelo no domínio do caso	Leitura	Domain*		
			Template*		
ListCaseRules	Concede permissão para listar regras de caso no domínio do caso	Lista	Domain*		
ListCasesForContact	Concede permissão para listar casos para um contato específico no domínio do caso	Lista	Domain*		
ListDomains	Concede permissão para listar todos os domínios em uma conta	Lista			
ListFieldOptions	Concede permissão para listar opções de campo para um único campo de seleção no domínio do caso	Lista	Domain*		
			Field*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListFields	Concede permissão para listar campos no domínio do caso	Lista	Domain*		
ListLayouts	Concede permissão para listar modelos no domínio do caso	Lista	Domain*		
ListTagsForResource	Concede permissão para listar as etiquetas para o recurso especificado	Leitura			
ListTemplates	Concede permissão para listar modelos no domínio do caso	Lista	Domain*		
PutCaseEventConfiguration	Concede permissão para inserir ou atualizar a configuração de evento do caso no domínio do caso	Gravar	Domain*		
SearchCases	Concede permissão para pesquisar casos no domínio do caso	Leitura	Domain*		
SearchRelatedItems	Concede permissão para criar itens associados ao caso no domínio do caso	Leitura	Case*		
			Domain*		
TagResource	Concede permissão para adicionar as etiquetas especificadas ao recurso especificado	Tags	Case		
			CaseRule		
			Domain		
			Field		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			Layout		
			RelatedItem		
			Template		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover as etiquetas especificadas do recurso especificado	Tags	Case		
			CaseRule		
			Domain		
			Field		
			Layout		
			RelatedItem		
			Template		
				aws:TagKeys	
UpdateCase	Concede permissão para atualizar valores de campos do caso no domínio do caso	Gravar	Case*		
			Domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			Field*		
				connect:UserArn	
UpdateCaseRule	Concede permissão para atualizar a regra do caso no domínio do caso	Gravar	CaseRule*		
			Domain*		
UpdateField	Concede permissão para atualizar o campo no domínio do caso	Gravar	Domain*		
			Field*		
UpdateLayout	Concede permissão para atualizar o layout no domínio do caso	Gravar	Domain*		
			Layout*		
UpdateTemplate	Concede permissão para atualizar o modelo no domínio do caso	Gravar	Domain*		
			Template*		

Tipos de recursos definidos pelo Amazon Connect Cases

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do Amazon Connect Cases

O Amazon Connect Cases define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves de etiqueta que são transmitidas na solicitação	ArrayOfString
connect:UserArn	Filtra o acesso por conexão UserArn	ARN

Ações, recursos e chaves de condição ao Amazon Connect Customer Profiles

O Amazon Connect Customer Profiles (prefixo de serviço: `profile`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em IAM políticas de permissão.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Connect Customer Profiles
- Tipos de recursos definidos pelo Amazon Connect Customer Profiles
- Chaves de condição para o Amazon Connect Customer Profiles

Ações definidas pelo Amazon Connect Customer Profiles

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddProfileKey	Concede permissão para adicionar uma chave de perfil	Gravar	domains*		
BatchGetCalculatedAttributeForProfile	Concede permissão para recuperar um atributo calculado dos perfis específicos no domínio	Leitura	calculated-attributes*		
			domains*		
BatchGetProfile	Concede permissão para obter perfis no domínio	Leitura	domains*		
CreateCalculatedAttributeDefinition	Concede permissão para criar uma definição de atributo calculado no domínio	Gravar	calculated-attributes*	aws:RequestTag/${TagKey} aws:TagKeys	
			domains*		
CreateDomain	Concede permissão para criar um domínio	Gravar	domains*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole
CreateDomainLayout	Concede permissão para criar um layout no domínio	Gravar	domains*		
			layouts*	aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
CreateEventStream	Concede permissão para colocar um fluxo de evento em um domínio	Gravar	domains*		iam:PutRolePolicy kinesis:DescribeStreamSummary
			event-streams*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventTrigger	Concede permissão para criar um gatilho de evento no domínio	Gravar	domains*		
			event-triggers*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateIntegrationWorkflow	Concede permissão para criar uma integração de fluxo de trabalho em um domínio	Gravar	domains*		
			integrations*	aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateProfile	Concede permissão para criar um perfil no domínio	Gravar	domains*		
CreateSegmentDefinition	Concede permissão para criar uma definição de segmento no domínio	Gravar	domains*		
			segment-definitions*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateSegmentEstimate	Concede permissão para criar uma estimativa de segmento no domínio	Gravar	domains*		
CreateSegmentSnapshot	Concede permissão para criar um snapshot de segmento no domínio	Gravar	domains*		
			segment-definitions*		
CreateSnapshot [somente permissão]	Concede permissão para criar um snapshot no domínio	Gravar	domains*		
CreateUploadJob	Concede permissão para criar um trabalho de upload no domínio	Gravar	domains*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteCalculatedAttributeDefinition	Concede permissão para excluir uma definição de atributo calculado no domínio	Gravar	calculated-attributes*		
			domains*		
DeleteDomain	Concede permissão para excluir um domínio	Gravar	domains*		
DeleteDomainLayout	Concede permissão para excluir um layout no domínio	Gravar	domains*		
			layouts*		
DeleteEventStream	Concede permissão para excluir um fluxo de evento em um domínio	Gravar	domains*		iam:DeleteRolePolicy
			event-streams*		
DeleteEventTrigger	Concede permissão para excluir um gatilho de evento no domínio	Gravar	domains*		
			event-triggers*		
DeleteIntegration	Concede permissão para excluir uma integração em um domínio	Gravação	domains*		
			integrations*		
DeleteProfile	Concede permissão para excluir um perfil	Gravação	domains*		
DeleteProfileKey	Concede permissão para excluir uma chave de perfil	Gravação	domains*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteProfileObject	Concede permissão para excluir um objeto de perfil	Gravação	domains*		
			object-types*		
DeleteProfileObjectType	Concede permissão para excluir um tipo de objeto de perfil específico no domínio	Gravar	domains*		
			object-types*		
DeleteSegmentDefinition	Concede permissão para excluir uma definição de segmento no domínio	Gravar	domains*		
			segment-definitions*		
DeleteWorkflow	Concede permissão para excluir um fluxo de trabalho em um domínio	Gravar	domains*		
DetectProfileObjectType	Concede permissões para detectar automaticamente o tipo de objeto	Leitura	domains*		
GetAutoMergingPreview	Concede permissão para obter uma previsualização da mesclagem automática em um domínio	Leitura	domains*		
GetCalculatedAttributeDefinition	Concede permissão para obter uma definição de atributo calculado no domínio	Leitura	calculated-attributes*		
			domains*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetCalculatedAttributeForProfile	Concede permissão para recuperar um atributo calculado para um perfil específico no domínio	Leitura	calculated-attributes*		
			domains*		
GetDomain	Concede permissão para obter um domínio específico em uma conta	Leitura	domains*		
GetDomainLayout	Concede permissão para obter um layout no domínio	Leitura	domains*		
			layouts*		
GetEventStream	Concede permissão para obter um fluxo de evento específico em um domínio	Leitura	domains*		kinesis:DescribeStreamSummary
			event-streams*		
GetEventTrigger	Concede permissão para obter um gatilho de evento no domínio	Leitura	domains*		
			event-triggers*		
GetIdentityResolutionJob	Concede permissão para obter uma tarefa de resolução de identidade em um domínio	Leitura	domains*		
GetIntegration	Concede permissão para obter integrações específicas em um domínio	Leitura	domains*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			integrations*		
GetMatches	Concede permissão para obter resultados de perfil em um domínio	Listar	domains*		
GetProfileObjectType	Concede permissão para obter um tipo de objeto de perfil específico no domínio	Leitura	domains*		
			object-types*		
GetProfileObjectTypeTemplate	Concede permissão para obter um modelo de tipo de objeto específico	Leitura			
GetSegmentDefinition	Concede permissão para obter uma definição de segmento no domínio	Leitura	domains*		
			segment-definitions*		
GetSegmentEstimate	Concede permissão para obter uma estimativa de segmento no domínio	Leitura	domains*		
GetSegmentMembership	Concede permissão para determinar se os perfis fornecidos fazem parte de um segmento no domínio	Leitura	domains*		
			segment-definitions*		
GetSegmentSnapshot		Leitura	domains*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	Concede permissão para obter o snapshot de um segmento no domínio		segment-definitions*		
GetSimilarProfiles	Concede permissão para obter todos os perfis semelhantes no domínio	Lista	domains*		
GetSnapshot [somente permissão]	Concede permissão para obter um snapshot no domínio	Leitura	domains*		
GetUploadJob	Concede permissão para obter detalhes de um trabalho de upload no domínio	Leitura	domains*		
GetUploadJobPath	Concede permissão para obter uma URL pré-assinada para fazer upload de arquivo para um trabalho de upload	Leitura	domains*		
GetWorkflow	Concede permissão para obter detalhes do fluxo de trabalho em um domínio	Leitura	domains*		
GetWorkflowSteps	Concede permissão para obter detalhes da etapa de fluxo de trabalho em um domínio	Leitura	domains*		
ListAccountIntegrations	Concede permissão para listar todas as integrações na conta	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListCalculatedAttributeDefinitions	Concede permissão para listar todas as definições de atributo calculado no domínio	Lista	domains*		
ListCalculatedAttributesForProfile	Concede permissão para listar todos os atributos calculados para um perfil específico no domínio	Lista	domains*		
ListDomainLayouts	Concede permissão para listar todos os layouts no domínio	Lista	domains*		
ListDomains	Concede permissão para listar todos os domínios em uma conta	Lista			
ListEventStreams	Concede permissão para listar todos os fluxos de evento em um domínio específico	Lista	domains*		
ListEventTriggers	Concede permissão para listar todos os acionadores de eventos no domínio	Lista	domains*		
ListIdentityResolutionJobs	Concede permissão para listar trabalhos de resolução de identidade em um domínio	Lista	domains*		
ListIntegrations	Concede permissão para listar todas as integrações em um domínio específico	Lista	domains*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListObjectTypeAttributes	Concede permissão para listar todos os atributos de um tipo de objeto específico no domínio	Lista	domains*		
			object-types*		
ListProfileAttributeValues	Concede permissão para listar todos os valores de um atributo de perfil no domínio	Lista	domains*		
ListProfileObjectTypeTemplates	Concede permissão para listar todos os modelos de tipo de objeto de perfil na conta	Listar			
ListProfileObjectTypes	Concede permissão para listar todos os tipos de objeto de perfil no domínio	Listar	domains*		
ListProfileObjects	Concede permissão para listar todos os objetos de perfil de um perfil	Lista	domains*		
			object-types*		
ListRuleBasedMatches	Concede permissão para listar todos os resultados de correspondência baseados em regras no domínio	Lista	domains*		
ListSegmentDefinitions	Concede permissão para listar todas as definições de segmento no domínio	Lista	domains*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	calculated-attributes		
			domains		
			event-streams		
			event-triggers		
			integrations		
			layouts		
			object-types		
			segment-definitions		
ListUploadJobs	Concede permissão para listar todos os trabalhos de upload no domínio	Lista	domains*		
ListWorkflows	Concede permissão para listar todos os fluxos de trabalho em um domínio específico	Lista	domains*		
MergeProfiles	Concede permissão para mesclar perfis em um domínio	Gravar	domains*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutIntegration	Concede permissão para colocar uma integração em um domínio	Gravação	domains*		
			integrations*	aws:RequestTag/${TagKey} aws:TagKeys	
PutProfileObject	Concede permissão para colocar um objeto para um perfil	Gravação	domains*		
			object-types*		
PutProfileObjectType	Concede permissão para colocar um tipo de objeto de perfil específico no domínio	Gravação	domains*		
			object-types*	aws:RequestTag/${TagKey} aws:TagKeys	
SearchProfiles	Concede permissão para pesquisar perfis em um domínio	Leitura	domains*		
StartUploadJob	Concede permissão para iniciar um trabalho de upload no domínio	Gravar	domains*		
StopUploadJob	Concede permissão para interromper um trabalho de upload no domínio	Gravar	domains*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para adicionar etiquetas a um recurso	Marcação	calculated-attributes		
			domains		
			event-streams		
			event-triggers		
			integrations		
			layouts		
			object-types		
			segment-definitions		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover etiquetas de um recurso	Tags	calculated-attributes		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			domains		
			event-streams		
			event-triggers		
			integrations		
			layouts		
			object-types		
			segment-definitions		
				aws:TagKeys	
UpdateCalculatedAttributeDefinition	Concede permissão para atualizar uma definição de atributo calculado no domínio	Gravar	calculated-attributes*		
			domains*		
UpdateDomain	Concede permissão para atualizar um domínio	Gravar	domains*		iam:CreateServiceLinkedRole
UpdateDomainLayout	Concede permissão para atualizar um layout no domínio	Gravar	domains*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			layouts*		
UpdateEventTrigger	Concede permissão para atualizar um gatilho de evento no domínio	Gravar	domains*		
			event-triggers*		
UpdateProfile	Concede permissão para atualizar um perfil no domínio	Gravação	domains*		

Tipos de recursos definidos pelo Amazon Connect Customer Profiles

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
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}

Chaves de condição para o Amazon Connect Customer Profiles

O Amazon Connect Customer Profiles define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma IAM política. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por uma chave presente na solicitação que o usuário faz ao serviço de Customer Profiles	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso por uma chave da etiqueta e par de valores	String
aws:TagKeys	Filtra o acesso pela lista de todos os nomes de chave da etiqueta presentes na solicitação que o usuário faz ao serviço de Customer Profiles	ArrayOfString

Ações, recursos e chaves de condição para campanhas externas do Amazon Connect

O Amazon Connect Outbound Campaigns (prefixo do serviço:`connect-campaigns`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelas campanhas externas do Amazon Connect
- Tipos de recursos definidos pelas campanhas externas do Amazon Connect
- Chaves de condição para campanhas externas do Amazon Connect

Ações definidas pelas campanhas externas do Amazon Connect

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateCampaign	Concede permissão para criar uma campanha	Gravar	campaign*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteCampaign	Concede permissão para excluir uma campanha	Gravar	campaign*		
DeleteCampaignChannelSubtypeConfig	Concede permissão para excluir a configuração do subtipo de canal de uma campanha	Gravar	campaign*		
DeleteCampaignCommunicationLimits	Concede permissão para excluir a configuração dos limites de comunicação de uma campanha	Gravar	campaign*		
DeleteCampaignCommunicationTime	Concede permissão para excluir a configuração do tempo de comunicação de uma campanha	Gravar	campaign*		
DeleteConnectInstanceConfig	Concede permissão para remover informações de configuração para uma instância do Amazon Connect	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteConnectInstanceIntegration	Concede permissão para remover informações de integração de uma instância do Amazon Connect	Gravar			
DeleteInstanceOnboardingJob	Concede permissão para remover um trabalho de integração para uma instância do Amazon Connect	Gravar			
DescribeCampaign	Concede permissão para descrever uma campanha específica	Leitura	campaign*		
				aws:RequestTag/${TagKey}	
GetCampaignState	Concede permissão para obter o estado de uma campanha	Leitura	campaign*		
				aws:RequestTag/${TagKey}	
GetCampaignStateBatch	Concede permissão para obter o estado das campanhas	Leitura	campaign*		
				aws:RequestTag/${TagKey}	
GetConnectInstanceConfig	Concede permissão para obter informações de configuração para uma instância do Amazon Connect	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetInstanceCommunicationLimits	Concede permissão para obter a configuração dos limites de comunicação de uma instância do Amazon Connect	Leitura			
GetInstanceOnboardingJobStatus	Concede permissão para obter o status de um trabalho de integração para uma instância do Amazon Connect	Leitura			
ListCampaigns	Concede permissão para fornecer um resumo de todas as campanhas	Lista		aws:RequestTag/${TagKey}	
ListConnectInstanceIntegrations	Concede permissão para fornecer um resumo de todas as integrações com uma instância do Amazon Connect	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	campaign		
				aws:ResourceTag/${TagKey}	
PauseCampaign	Concede permissão para pausar uma campanha	Gravar	campaign*		
PutConnectInstanceIntegration	Concede permissão para colocar uma configuração de integração com uma instância do Amazon Connect	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutDialRequestBatch	Concede permissão para criar solicitações de discagem para a campanha especificada	Gravar	campaign*		
PutInstanceCommunicationLimits	Concede permissão para definir a configuração dos limites de comunicação de uma instância do Amazon Connect	Gravar			
PutOutboundRequestBatch	Concede permissão para criar solicitações de discagem para a campanha especificada	Gravar	campaign*		
PutProfileOutboundRequestBatch	Concede permissão para criar solicitações externas de perfil para a campanha especificada	Gravar	campaign*		
ResumeCampaign	Concede permissão para retomar uma campanha	Gravar	campaign*		
StartCampaign	Concede permissão para iniciar uma campanha	Gravar	campaign*		
StartInstanceOnboardingJob	Concede permissão para iniciar um trabalho de integração para uma instância do Amazon Connect	Gravar			
StopCampaign	Concede permissão para interromper uma campanha	Gravar	campaign*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para marcar um recurso	Marcação	campaign*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para desmarcar um recurso	Tags	campaign*		
				aws:TagKeys	
UpdateCampaignChannelSubtypeConfig	Concede permissão para atualizar a configuração do subtipo de canal de uma campanha	Gravar	campaign*		
UpdateCampaignCommunicationLimits	Concede permissão para atualizar a configuração dos limites de comunicação de uma campanha	Gravar	campaign*		
UpdateCampaignCommunicationTime	Concede permissão para atualizar a configuração do tempo de comunicação de uma campanha	Gravar	campaign*		
UpdateCampaignDialerConfig	Concede permissão para atualizar a configuração de discador de uma campanha	Gravar	campaign*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateCampaignFlowAssociation	Concede permissão para atualizar a associação de fluxo de uma campanha	Gravar	campaign*		
UpdateCampaignName	Concede permissão para atualizar o nome de uma campanha	Gravar	campaign*		
UpdateCampaignOutboundCallConfig	Concede permissão para atualizar a configuração de uma ligação de saída de uma campanha	Gravar	campaign*		
UpdateCampaignSchedule	Concede permissão para atualizar o cronograma de uma campanha	Gravar	campaign*		
UpdateCampaignSource	Concede permissão para atualizar a fonte de uma campanha	Gravar	campaign*		

Tipos de recursos definidos pelas campanhas externas do Amazon Connect

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
campaign	`arn:${Partition}:connect-campaigns:${Region}:${Account}:campaign/${CampaignId}`	aws:ResourceTag/${TagKey}

Chaves de condição para campanhas externas do Amazon Connect

O Amazon Connect Outbound Campaigns define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por ações com base na presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por ações com base nos pares de chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso por ações com base na presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o Amazon Connect Voice ID

O Amazon Connect Voice ID. (prefixo do serviço: `voiceid`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Connect Voice ID
- Tipos de recursos definidos pelo Amazon Connect Voice ID
- Chaves de condição para o Amazon Connect Voice ID

Ações definidas pelo Amazon Connect Voice ID

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de

condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateFraudster	Concede permissão para associar um fraudador a uma lista de observações	Gravar	domain*		
CreateDomain	Concede permissão para criar um domínio	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWatchlist	Concede permissão para criar uma lista de observação	Gravar	domain*		
DeleteDomain	Concede permissão para excluir um domínio	Gravar	domain*		
DeleteFraudster	Concede permissão para excluir um fraudador	Gravar	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteSpeaker	Concede permissão para excluir um palestrante	Gravar	domain*		
DeleteWatchlist	Concede permissão para excluir uma lista de observação	Gravar	domain*		
DescribeComplianceConsent [somente permissão]	Concede permissão para descrever consentimento de conformidade	Leitura			
DescribeDomain	Concede permissão para descrever um domínio	Leitura	domain*		
DescribeFraudster	Concede permissão para descrever um fraudador	Leitura	domain*		
DescribeFraudsterRegistrationJob	Concede permissão para descrever um trabalho de registro de fraudador	Leitura	domain*		
DescribeSpeaker	Concede permissão para descrever um palestrante	Leitura	domain*		
DescribeSpeakerEnrollmentJob	Concede permissão para descrever um job de inscrição de palestrante	Leitura	domain*		
DescribeWatchlist	Concede permissão para descrever uma lista de observação	Leitura	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateFraudster	Concede permissão para desassociar um fraudador de uma lista de observações	Gravar	domain*		
EvaluateSession	Concede permissão para criar uma sessão	Gravar	domain*		
ListDomains	Concede permissão para listar domínios para uma conta	Lista			
ListFraudsterRegistrationJobs	Concede permissão para listar trabalhos de registro de fraudadores para um domínio	Lista	domain*		
ListFraudsters	Concede permissão para listar fraudadores para um domínio ou uma lista de observações	Lista	domain*		
ListSpeakerEnrollmentJobs	Concede permissão para listar trabalhos de registro de palestrantes para um domínio	Lista	domain*		
ListSpeakers	Concede permissão para listar palestrantes para um domínio	Lista	domain*		
ListTagsForResource	Concede permissão para listar etiquetas para um recurso do Voice ID	Leitura	domain		
ListWatchlists	Concede permissão para listar listas de observação para um domínio	Lista	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
OptOutSpeaker	Concede permissão para excluir um palestrante	Gravar	domain*		
RegisterComplianceConsent [somente permissão]	Concede permissão para registrar consentimento de conformidade	Gravar			
StartFraudsterRegistrationJob	Concede permissão para iniciar um trabalho de registro de fraudador	Gravar	domain*		
StartSpeakerEnrollmentJob	Concede permissão para iniciar um trabalho de inscrição de palestrante	Gravar	domain*		
TagResource	Concede permissão para listar marcar um recurso do Voice ID	Tags	domain		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover uma etiqueta de um recurso do Voice ID	Tags	domain		
				aws:TagKeys	
UpdateDomain	Concede permissão para atualizar um domínio	Gravar	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateWatchlist	Concede permissão para atualizar uma lista de observações	Gravar	domain*		

Tipos de recursos definidos pelo Amazon Connect Voice ID

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
domain	`arn:${Partition}:voiceid:${Region}:${Account}:domain/${DomainId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o Amazon Connect Voice ID

O Amazon Connect Voice ID define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves de etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Connector Service

AWS O Connector Service (prefixo do serviço:`awsconnector`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Connector Service
- Tipos de recursos definidos pelo AWS Connector Service
- Chaves de condição do AWS Connector Service

Ações definidas pelo AWS Connector Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou

ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetConnectorHealth [somente permissão]	Recupera todas as métricas de integridade publicadas no Server Migration Connector.	Read			
RegisterConnector [somente permissão]	Registra o AWS conector com o AWS Connector Service.	Gravar			
ValidateConnectorId [somente permissão]	Valida a ID do conector de migração do servidor que foi registrada no AWS Connector Service.	Leitura			

Tipos de recursos definidos pelo AWS Connector Service

AWS O Connector Service não suporta a especificação de um ARN de recurso no elemento de uma `Resource` declaração de política do IAM. Para conceder acesso ao AWS Connnector Service, especifique `"Resource": "*"` na política.

Chaves de condição do AWS Connector Service

O Connector Service não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Management Console Mobile App

AWS Management Console O aplicativo móvel (prefixo do serviço:`consoleapp`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Management Console Mobile App
- Tipos de recursos definidos pelo AWS Management Console Mobile App
- Chaves de condição do AWS Management Console Mobile App

Ações definidas pelo AWS Management Console Mobile App

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa

ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetDeviceIdentity	Concede permissão para recuperar a identidade de dispositivo para um dispositivo Console Mobile App	Leitura	DeviceIdentity*		
ListDeviceIdentities	Concede permissão para recuperar uma lista de identidades de dispositivos	Lista			

Tipos de recursos definidos pelo AWS Management Console Mobile App

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
DeviceIdentity	`arn:${Partition}:consoleapp::${Account}:device/${DeviceId}/identity/${IdentityId}`	

Chaves de condição do AWS Management Console Mobile App

O aplicativo móvel do console não tem chaves de contexto específicas do serviço que possam ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o AWS Consolidated Billing

AWS O faturamento consolidado (prefixo do serviço:`consolidatedbilling`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Consolidated Billing

- Tipos de recursos definidos pelo AWS Consolidated Billing
- Chaves de condição para o AWS Consolidated Billing

Ações definidas pelo AWS Consolidated Billing

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAccountBillingRole [somente permissão]	Concede permissão para obter o perfil de conta (pagador, vinculado, comum)	Leitura			
ListLinkedAccounts [somente permissão]	Concede permissão para obter uma lista de member/linked contas	Lista			

Tipos de recursos definidos pelo AWS Consolidated Billing

AWS O faturamento consolidado não é compatível com a especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para conceder acesso ao AWS Consolidated Billing, especifique `"Resource": "*"` em sua política.

Chaves de condição para o AWS Consolidated Billing

O Consolidated Billing não tem chaves de contexto específicas do serviço que possam ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Control Catalog

AWS O Control Catalog (prefixo do serviço:`controlcatalog`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Control Catalog
- Tipos de recurso definidos pelo AWS Control Catalog
- Chaves de condição do AWS Control Catalog

Ações definidas pelo AWS Control Catalog

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetControl	Concede permissão para retornar detalhes sobre um controle específico	Leitura	control*		
ListCommonControls	Concede permissão para retornar uma lista paginada de controles comuns do AWS Catálogo de Controle	Lista			
ListControlMappings	Concede permissão para retornar uma lista paginada de mapeamentos de controle do Catálogo de Controle AWS	Lista			
ListControls	Concede permissão para retornar uma lista paginada de todos os controles disponíve	Lista	control*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	is na biblioteca do Catálogo AWS de Controle				
ListDomains	Concede permissão para retornar uma lista paginada de domínios do Catálogo de Controle AWS	Lista			
ListObjectives	Concede permissão para retornar uma lista paginada de objetivos do Catálogo de Controle AWS	Lista			

Tipos de recurso definidos pelo AWS Control Catalog

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
common-control	`arn:${Partition}:controlcatalog:::common-control/${CommonControlId}`	
control	`arn:${Partition}:controlcatalog:::control/${ControlId}`	

Tipos de recursos	ARN	Chaves de condição
domain	`arn:${Partition}:controlcatalog:::domain/${DomainId}`	
objective	`arn:${Partition}:controlcatalog:::objective/${ObjectiveId}`	

Chaves de condição do AWS Control Catalog

O Control Catalog não tem chaves de contexto específicas do serviço que podem ser usadas no elemento `Condition` das instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Control Tower

AWS O Control Tower (prefixo do serviço:`controltower`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Control Tower
- Tipos de recurso definidos pelo AWS Control Tower
- Chaves de condição do AWS Control Tower

Ações definidas pelo AWS Control Tower

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou

ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateLandingZone	Concede permissão para criar uma zona de pouso	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	controltower:TagResource
CreateManagedAccount [somente permissão]	Concede permissão para criar uma conta gerenciada pela AWS Control Tower	Gravar			
DeleteLandingZone	Concede permissão para excluir a landing zone da AWS Control Tower	Gravar	LandingZone*		
DeregisterManagedAccount [somente permissão]	Concede permissão para cancelar o registro de uma conta criada por meio da fábrica de contas da Control Tower AWS	Gravar			
DeregisterOrganizationalUnit [somente permissão]	Concede permissão para cancelar o registro de uma unidade organizacional na gerência da AWS Control Tower	Gravar			
DescribeAccountFactoryConfig [somente permissão]	Concede permissão para descrever a configuração atual do Account Factory	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeCoreService [somente permissão]	Concede permissão para descrever recursos gerenciados pelas contas principais na AWS Control Tower	Leitura			
DescribeGuardrail [somente permissão]	Concede permissão para descrever uma barreira de proteção	Leitura			
DescribeGuardrailForTarget [somente permissão]	Concede permissão para descrever uma barreira de proteção de uma unidade organizacional	Leitura			
DescribeLandingZoneConfiguration [somente permissão]	Concede permissão para descrever a configuração atual da zona de pouso	Leitura			
DescribeManagedAccount [somente permissão]	Concede permissão para descrever uma conta criada pelo Account Factory	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeManagedOrganizationalUnit [somente permissão]	Concede permissão para descrever uma unidade organizacional da AWS Organizations gerenciada pela AWS Control Tower	Leitura			
DescribeRegisterOrganizationalUnitOperation [somente permissão]	Concede permissão para descrever uma operação de unidade operacional de registro	Leitura			
DescribeSingleSignOn [somente permissão]	Concede permissão para descrever a configuração atual do AWS Control Tower IAM Identity Center	Leitura			
DisableBaseline	Concede permissão para desabilitar uma linha de base em um destino	Gravar	EnabledBaseline*		
DisableControl	Concede permissão para remover um controle de uma unidade organizacional	Gravar	EnabledControl*		
DisableGuardrail [somente permissão]	Concede permissão para desabilitar uma barreira de proteção de uma unidade organizacional	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
EnableBaseline	Concede permissão para habilitar uma linha de base em um destino	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	controltower:TagResource
EnableControl	Concede permissão para ativar um controle para uma unidade organizacional	Gravar	EnabledControl		controltower:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
EnableGuardrail [somente permissão]	Concede permissão para habilitar uma barreira de proteção de uma unidade organizacional	Gravar			
GetAccountInfo [somente permissão]	Concede permissão para descrever um e-mail de conta e validar que ele existe	Leitura			
GetAvailableUpdates [somente permissão]	Concede permissão para listar as atualizações disponíveis para a implantação atual do AWS Control Tower	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetBaseline	Concede permissão para obter detalhes da linha de base	Leitura	Baseline*		
GetBaselineOperation	Concede permissão para obter o status atual de uma determinada operação de linha de base	Leitura			
GetControlOperation	Concede permissão para obter o status atual de uma determinada DisableControl operação EnabledControl ou operação	Leitura			
GetEnabledBaseline	Concede permissão para obter uma linha de base habilitada	Leitura	EnabledBaseline*		
GetEnabledControl	Concede permissão para obter um controle habilitado de uma unidade organizacional	Leitura	EnabledControl*		
GetGuardrailComplianceStatus [somente permissão]	Concede permissão para obter o status atual de conformidade de uma barreira de proteção	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetHomeRegion [somente permissão]	Concede permissão para obter a região de origem da configuração da AWS Control Tower	Leitura			
GetLandingZone	Concede permissão para obter o status atual da configuração da zona de pouso	Leitura	LandingZone*		
GetLandingZoneDriftStatus	Concede permissão para obter o status atual da oscilação da zona de pouso	Leitura			
GetLandingZoneOperation	Concede permissão para obter o status atual de uma operação de zona de pouso	Leitura			
GetLandingZoneStatus [somente permissão]	Concede permissão para obter o status atual da configuração da zona de pouso	Leitura			
ListBaselines	Concede permissão para listar linhas de base	Lista			
ListControlOperations	Concede permissão para listar todas as operações de controle	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDirectoryGroups [somente permissão]	Concede permissão para listar os grupos atuais de diretórios disponíveis por meio do Centro de Identidade do IAM	Lista			
ListDriftDetails	Concede permissão para listar ocorrências de deriva na AWS Control Tower	Leitura			
ListEnabledBaselines	Concede permissão para listar linhas de base habilitadas	Lista			
ListEnabledControls	Concede permissão para listar todos os controles habilitados em uma unidade organizacional especificada	Lista			
ListEnabledGuardrails [somente permissão]	Concede permissão para listar barreiras de proteção habilitadas atualmente	Lista			
ListExtendGovernancePrecheckDetails [somente permissão]	Concede permissão para listar detalhes de pré-verificação em uma unidade organizacional	Lista			
ListExternalConfigRuleCompliance	Concede permissão para listar a conformidade das regras externas do AWS Config	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListGuardrailViolations [somente permissão]	Concede permissão para listar violações de barreira de proteção existentes	Lista			
ListGuardrails [somente permissão]	Concede permissão para listar todas as barreiras de proteção disponíveis	Lista			
ListGuardrailsForTarget [somente permissão]	Concede permissão para listar as barreiras de proteção de uma unidade organizacional e o estado atual delas	Lista			
ListLandingZoneOperations	Concede permissão para listar todas as operações da zona de pouso	Lista			
ListLandingZones	Concede permissão para listar todas as zonas de pouso	Lista			
ListManagedAccounts [somente permissão]	Concede permissão para listar contas gerenciadas pela AWS Control Tower	Lista			
ListManagedAccountsForGuardrail [somente permissão]	Concede permissão para listar as contas gerenciadas com uma barreira de proteção específica aplicada	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListManagedAccountsForParent [somente permissão]	Concede permissão para listar as contas gerenciadas de uma unidade organizacional	Lista			
ListManagedOrganizationalUnits [somente permissão]	Concede permissão para listar unidades organizacionais gerenciadas pela AWS Control Tower	Lista			
ListManagedOrganizationalUnitsForGuardrail [somente permissão]	Concede permissão para listar as unidades organizacionais gerenciadas que têm uma barreira de proteção específica aplicada	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	EnabledBaseline		
			EnabledControl		
			LandingZone		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ManageOrganizationalUnit [somente permissão]	Concede permissão para configurar uma unidade organizacional a ser gerenciada pela AWS Control Tower	Gravar			
PerformPreLaunchChecks [somente permissão]	Concede permissão para realizar validações em uma conta	Leitura			
ResetEnabledBaseline	Concede permissão para redefinir uma linha de base habilitada	Gravar	EnabledBaseline*		
ResetEnabledControl	Concede permissão para redefinir um controle ativado para uma unidade organizacional	Gravar	EnabledControl*		
ResetLandingZone	Concede permissão para redefinir uma zona de pouso	Gravar	LandingZone*		
SetupLandingZone [somente permissão]	Concede permissão para configurar ou atualizar a landing zone da AWS Control Tower	Gravar			
TagResource	Concede permissão para adicionar tags a um recurso	Marcação	EnabledBaseline		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			EnabledControl		
			LandingZone		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover etiquetas de um recurso	Tags	EnabledBaseline		
			EnabledControl		
			LandingZone		
				aws:TagKeys	
UpdateAccountFactoryConfig [somente permissão]	Concede permissão para atualizar a configuração do Account Factory	Gravar			
UpdateEnabledBaseline	Concede permissão para atualizar uma linha de base habilitada	Gravar	EnabledBaseline*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateEnabledControl	Concede permissão para atualizar um controle habilitado para uma unidade organizacional	Gravar	EnabledControl*		
UpdateLandingZone	Concede permissão para atualizar uma zona de pouso	Gravar	LandingZone*		

Tipos de recurso definidos pelo AWS Control Tower

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Tipos de recursos	ARN	Chaves de condição
LandingZone	`arn:${Partition}:controltower:${Region}:${Account}:landingzone/${LandingZoneId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Control Tower

AWS A Control Tower define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Cost and Usage Report

AWS O relatório de custo e uso (prefixo do serviço:`cur`) fornece os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Cost and Usage Report
- Tipos de recursos definidos pelo AWS Cost and Usage Report
- Chaves de condição do AWS Cost and Usage Report

Ações definidas pelo AWS Cost and Usage Report

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de

condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteReportDefinition	Concede permissão para excluir a definição do Relatório de Custos e Uso	Gravar	cur*		
DescribeReportDefinitions	Concede permissão para obter as definições do Relatório de Custos e Uso	Leitura			
GetClassicReport [somente permissão]	Concede permissão para obter o relatório CSV de faturas	Leitura			
GetClassicReportPreferences [somente permissão]	Concede permissão para obter o status de ativação de relatórios clássico para os Relatórios de Uso	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetUsageReport [somente permissão]	Concede permissão para obter uma lista de AWS serviços, tipo de uso e operação para o fluxo de trabalho do Relatório de Uso. Também permite ou nega o download de relatórios de uso	Leitura			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	cur*		
				aws:ResourceTag/${TagKey}	
ModifyReportDefinition	Concede permissão para modificar a definição do Relatório de Custos e Uso	Gravar	cur*		
PutClassicReportPreferences [somente permissão]	Concede permissão para habilitar relatórios clássicos	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutReportDefinition	Concede permissão para gravar a definição do Relatório de Custos e Uso	Gravar	cur*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
TagResource	Concede permissão para marcar um recurso	Marcação	cur*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permissão para desmarcar um recurso	Marcação	cur*		
				aws:TagKeys aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ValidateReportDestination [somente permissão]	Concede permissão para validar se o bucket do s3 existe com as permissões adequadas para a entrega do CUR	Leitura			

Tipos de recursos definidos pelo AWS Cost and Usage Report

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
cur	`arn:${Partition}:cur:${Region}:${Account}:definition/${ReportName}`	

Chaves de condição do AWS Cost and Usage Report

AWS O relatório de custo e uso define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Cost Explorer Service

AWS O Cost Explorer Service (prefixo do serviço:`ce`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Cost Explorer Service
- Tipos de recursos definidos pelo AWS Cost Explorer Service
- Chaves de condição do AWS Cost Explorer Service

Ações definidas pelo AWS Cost Explorer Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAnomalyMonitor	Concede permissão para criar um monitor de anomalia	Gravação		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAnomalySubscription	Concede permissão para criar uma assinatura de anomalia	Gravação		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCostCategoryDefinition	Concede permissão para criar uma Cost Category com o nome e as regras solicitadas	Gravação		aws:RequestTag/${TagKey} aws:TagKeys	
CreateNotificationSubscription [somente permissão]	Concede permissão para criar alertas de expiração de reserva	Gravação			
CreateReport [somente permissão]	Concede permissão para criar relatórios do Cost Explorer	Gravação			
DeleteAnomalyMonitor	Concede permissão para excluir um monitor de anomalia	Gravação	anomalymonitor*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
DeleteAnomalySubscription	Concede permissão para excluir uma assinatura de anomalia	Gravação	anomalysubscription*		
				aws:ResourceTag/${TagKey}	
DeleteCostCategoryDefinition	Concede permissão para excluir uma Cost Category.	Gravação	costcategory*		
				aws:ResourceTag/${TagKey}	
DeleteNotificationSubscription [somente permissão]	Concede permissão para excluir alertas de expiração de reserva	Gravação			
DeleteReport [somente permissão]	Concede permissão para excluir relatórios do Cost Explorer	Gravação			
DescribeCostCategoryDefinition	Concede permissão para recuperar descrições, como nome, ARN, regras, definição e datas de efetivação de uma Cost Category	Leitura	costcategory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
DescribeNotificationSubscription [somente permissão]	Concede permissão para exibir alertas de expiração de reserva	Leitura			
DescribeReport [somente permissão]	Concede permissão para exibir a página de relatórios do Cost Explorer	Leitura			
GetAnomalies	Concede permissão para recuperar anomalias	Leitura	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
GetAnomalyMonitors	Concede permissão para consultar monitores de anomalia	Leitura	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
GetAnomalySubscriptions	Concede permissão para consultar assinaturas de anomalia	Leitura	anomalysubscription*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
GetApproximateUsageRecords	Concede permissão para recuperar a contagem aproximada de registros de uso para as escolhas de recursos, níveis e as preferências de granularidade por hora, derivados do uso do mês anterior	Leitura			
GetCommitmentPurchaseAnalysis	Concede permissão para recuperar a análise de compra comprometida de sua conta	Leitura			
GetConsoleActionSetEnforced [somente permissão]	Concede permissão para visualizar se ações do IAM existentes ou refinadas estão sendo usadas para controlar a autorização para os consoles de Faturamento, Gerenciamento de Custos e Contas	Leitura			
GetCostAndUsage	Concede permissão para recuperar os custos e as métricas de uso de sua conta	Leitura	billingview		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetCostAndUsageComparisons	Concede permissão para recuperar as comparações de custo e uso da sua conta	Leitura	billingview		
				aws:ResourceTag/${TagKey}	
GetCostAndUsageWithResources	Concede permissão para recuperar os custos e as métricas de uso com recursos de sua conta	Leitura	billingview		
				aws:ResourceTag/${TagKey}	
GetCostCategories	Concede permissão para consultar nomes e valores da Categoria de custos para um período especificado	Leitura	billingview		
				aws:ResourceTag/${TagKey}	
GetCostComparisonDrivers	Concede permissão para recuperar os fatores de custo da sua conta	Leitura	billingview		
				aws:ResourceTag/${TagKey}	
GetCostForecast	Concede permissão para recuperar uma previsão de custos para um período previsto	Leitura	billingview		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetDimensionValues	Concede permissão para recuperar todos os valores de filtro disponíveis para um filtro por um período	Leitura	billingview		
				aws:ResourceTag/${TagKey}	
GetPreferences [somente permissão]	Concede permissão para exibir a página de preferências do Cost Explorer	Leitura			
GetReservationCoverage	Concede permissão para recuperar a cobertura de reserva de sua conta	Leitura			
GetReservationPurchaseRecommendation	Concede permissão para recuperar as recomendações de reserva de sua conta	Leitura			
GetReservationUtilization	Concede permissão para recuperar a utilização de reserva de sua conta	Leitura			
GetRightsizingRecommendation	Concede permissão para recuperar as recomendações de redimensionamento de sua conta	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSavingsPlanPurchaseRecommendationDetails	Concede permissão para recuperar os detalhes de recomendação do Savings Plan para sua conta	Leitura			
GetSavingsPlansCoverage	Concede permissão para recuperar a cobertura dos Savings Plans de sua conta	Leitura			
GetSavingsPlansPurchaseRecommendation	Concede permissão para recuperar as recomendações de Savings Plans de sua conta	Leitura			
GetSavingsPlansUtilization	Concede permissão para recuperar a utilização de Savings Plans de sua conta	Leitura			
GetSavingsPlansUtilizationDetails	Concede permissão para recuperar os detalhes de utilização de Savings Plans de sua conta	Leitura			
GetTags	Concede permissão para consultar as etiquetas de um período especificado	Leitura	billingview		
				aws:ResourceTag/${TagKey}	
GetUsageForecast	Concede permissão para recuperar uma previsão de uso de um período previsto	Leitura	billingview		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
ListCommitmentPurchaseAnalyses	Concede permissão para recuperar uma lista de suas análises históricas de compromissos de compra	Lista			
ListCostAllocationTagBackfillHistory	Concede permissão para listar o histórico de preenchimento da tag de alocação de custos	Lista			
ListCostAllocationTags	Concede permissões para listar etiquetas de alocação de custo	Lista			
ListCostCategoryDefinitions	Concede permissão para recuperar nomes, ARN e datas de efetivação de todas as Cost Categories	Lista			
ListSavingsPlansPurchaseRecommendationGeneration	Concede permissão para recuperar uma lista de suas gerações de recomendações históricas	Lista			
ListTagsForResource	Concede permissão para listar etiquetas de um recurso do Cost Explorer	Leitura	anomalymonitor		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			anomalysubscription		
			costcategory		
				aws:ResourceTag/${TagKey}	
ProvideAnomalyFeedback	Concede permissão para fornecer feedback sobre anomalias detectadas	Gravar			
StartCommitmentPurchaseAnalysis	Concede permissão para solicitar uma análise de compra por compromisso	Gravar			
StartCostAllocationTagBackfill	Concede permissão para solicitar um preenchimento da tag de alocação de custos	Gravar			
StartSavingsPlansPurchaseRecommendationGeneration	Concede permissão para solicitar uma geração de recomendações de Savings Plans	Gravar			
TagResource	Concede permissão para etiquetar um recurso do Cost Explorer	Tags	anomalymonitor		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			anomalysubscription		
			costcategory		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permissão para remover etiquetas de um recurso do Cost Explorer	Tags	anomalymonitor		
			anomalysubscription		
			costcategory		
				aws:TagKeys aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateAnomalyMonitor	Concede permissão para atualizar um monitor de anomalia existente	Gravação	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
UpdateAnomalySubscription	Concede permissão para atualizar uma assinatura de anomalia existente	Gravar	anomalysubscription*		
				aws:ResourceTag/${TagKey}	
UpdateConsoleActionSetEnforced [somente permissão]	Concede permissão para alterar se ações do IAM existentes ou refinadas serão usadas para controlar a autorização para os consoles de Faturamento, Gerenciamento de Custos e Contas	Gravar			
UpdateCostAllocationTagsStatus	Concede permissão para atualizar o status de etiquetas existentes de alocação de custos	Gravar			
UpdateCostCategoryDefinition	Concede permissão para atualizar uma Cost Category existente	Gravação	costcategory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
UpdateNotificationSubscription [somente permissão]	Concede permissão para atualizar alertas de expiração de reserva	Gravação			
UpdatePreferences [somente permissão]	Concede permissão para editar a página de preferências do Cost Explorer	Gravação			
UpdateReport [somente permissão]	Concede permissão para atualizar os relatórios do Cost Explorer	Gravação			

Tipos de recursos definidos pelo AWS Cost Explorer Service

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS Cost Explorer Service

AWS O Cost Explorer Service define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Hub de Otimização de Custos da AWS

AWS O Cost Optimization Hub (prefixo do serviço:`cost-optimization-hub`) fornece os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Hub de Otimização de Custos da AWS
- Tipos de recursos definidos pelo Hub de Otimização de Custos da AWS
- Chaves de condição para o Hub de Otimização de Custos da AWS

Ações definidas pelo Hub de Otimização de Custos da AWS

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa

ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetPreferences	Concede permissão para obter preferências	Leitura			
GetRecommendation	Concede permissão para obter a configuração de recursos e o impacto estimado do custo de uma recomendação	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListEnrollmentStatuses	Concede permissão para listar status de inscrição da conta especificada ou de todos os membros em uma conta de gerenciamento	Lista			
ListRecommendationSummaries	Concede permissão para listar resumos de recomendações por grupo	Lista			cost-optimization-hub:GetRecommendation
ListRecommendations	Concede permissão para listar a visualização de resumo das recomendações	Lista			cost-optimization-hub:GetRecommendation
UpdateEnrollmentStatus	Concede permissão para atualizar o status de inscrição.	Gravar			
UpdatePreferences	Concede permissão para atualizar preferências	Gravar			

Tipos de recursos definidos pelo Hub de Otimização de Custos da AWS

AWS O Cost Optimization Hub não suporta a especificação de um ARN de recurso `Resource` no elemento de uma declaração de política do IAM. Para conceder acesso ao Hub de Otimização de Custos da AWS , especifique `"Resource": "*"` na sua política.

Chaves de condição para o Hub de Otimização de Custos da AWS

O Hub de Otimização de Custos não possui chaves de contexto específicas do serviço que possam ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o AWS Customer Verification Service

AWS O Serviço de Verificação do Cliente (prefixo do serviço:`customer-verification`) fornece os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Customer Verification Service
- Tipos de recursos definidos pelo AWS Customer Verification Service
- Chaves de condição para o AWS Customer Verification Service

Ações definidas pelo AWS Customer Verification Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o

nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateCustomerVerificationD	Concede permissão para criar dados de verificação do cliente	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
etails [somente permissão]					
CreateUploadUrls [somente permissão]	Concede permissão para criar upload URLs	Gravar			
GetCustomerVerificationDetails [somente permissão]	Concede permissão para obter dados de verificação do cliente	Leitura			
GetCustomerVerificationEligibility [somente permissão]	Concede permissão para obter a elegibilidade de verificação do cliente	Leitura			
UpdateCustomerVerificationDetails [somente permissão]	Concede permissão para atualizar dados de verificação do cliente	Gravar			

Tipos de recursos definidos pelo AWS Customer Verification Service

AWS O Serviço de verificação do cliente não suporta a especificação de um ARN de recurso no elemento de uma `Resource` declaração de política do IAM. Para conceder acesso ao AWS Customer Verification Service, especifique `"Resource": "*"` na política.

Chaves de condição para o AWS Customer Verification Service

O Customer Verification Service não tem chaves de contexto específicas ao serviço capazes de ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Data Exchange

AWS O Data Exchange (prefixo do serviço:`dataexchange`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Data Exchange
- Tipos de recursos definidos pelo AWS Data Exchange
- Chaves de condição do AWS Data Exchange

Ações definidas pelo AWS Data Exchange

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptDataGrant	Concede permissão para aceitar uma concessão de dados	Gravar	data-grants*		
CancelJob	Concede permissão para cancelar um trabalho	Gravar	jobs*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAsset [somente permissão]	Concede permissão para criar um ativo (por exemplo, em um trabalho)	Gravar	revisions*		
CreateDataGrant	Concede permissão para criar uma concessão de dados	Gravar	data-grants*		dataexchange:PublishToDataGrant
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSet	Concede permissão para criar um conjunto de dados	Gravar	data-sets*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventAction	Concede permissão para criar uma ação de evento	Gravar	event-actions*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateJob	Concede permissão para criar um trabalho para importar ou exportar ativos	Gravar	jobs*		
				dataexchange:JobType	
CreateRevision	Concede permissão para criar uma revisão	Gravar	data-sets*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAsset	Concede permissão para excluir um ativo	Gravar	assets*		
DeleteDataGrant	Concede permissão para excluir uma concessão de dados	Gravar	data-grants*		
DeleteDataSet	Concede permissão para excluir um conjunto de dados	Gravar	data-sets*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			entitled-data-sets*		
DeleteEventAction	Concede permissão para excluir uma ação de evento	Gravar	event-actions*		
DeleteRevision	Concede permissão para excluir uma revisão	Gravar	revisions*		
GetAsset	Concede permissão para obter informações sobre um ativo e exportá-la (por exemplo, em um trabalho)	Leitura	assets*		
			entitled-assets*		
GetDataGrant	Concede permissão para obter uma concessão de dados	Leitura	data-grants*		
GetDataSet	Concede permissão para obter informações sobre um conjunto de dados	Leitura	data-sets*		
			entitled-data-sets*		
GetEventAction	Concede permissão para obter uma ação de evento	Leitura	event-actions*		
GetJob	Concede permissão para obter informações sobre um trabalho	Leitura	jobs*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetReceivedDataGrant	Concede permissão para obter uma concessão de dados recebido	Leitura	data-grants*		
GetRevision	Concede permissão para obter informações sobre uma revisão	Leitura	entitled-revisions*		
			revisions*		
ListDataGrants	Concede permissão para listar concessões de dados para a conta	Lista			
ListDataSetRevisions	Concede permissão para listar as revisões de um conjunto de dados	Lista	data-sets*		
			entitled-data-sets*		
ListDataSets	Concede permissão para listar os conjuntos de dados para a conta	Lista			
ListEventActions	Concede permissão para listar ações de evento para a conta	Lista			
ListJobs	Concede permissão para listar trabalhos para a conta	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListReceivedDataGrants	Concede permissão para listar concessões de dados recebidas na conta	Lista			
ListRevisionAssets	Concede permissão para obter a lista dos ativos de uma revisão	Lista	entitled-revisions *		
			revisions *		
ListTagsForResource	Concede permissão para listar as etiquetas associadas ao recurso especificado	Lista	data-grants		
			data-sets		
			event-actions		
			revisions		
PublishDataSet [somente permissão]	Concede permissão para publicar um conjunto de dados em um produto	Gravar	data-sets *		
PublishToDataGrant [somente permissão]	Concede permissão para publicar um conjunto de dados em uma concessão de dados	Gravar	data-sets *		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
RevokeRevision	Concede permissão para revogar o acesso de assinante a uma revisão	Gravar	revisions*		
SendApiAsset	Concede permissão para enviar uma solicitação a um ativo do API	Gravar	assets*		
			entitled-assets*		
SendDataSetNotification	Concede permissão para enviar uma notificação para os assinantes de um conjunto de dados	Gravar	data-sets*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartJob	Concede permissão para iniciar um trabalho	Gravar	jobs*		dataexchange:CreateAsset dataexchange:DeleteDataSet dataexchange:GetAsset dataexchange:GetDataSet dataexchange:GetRevision dataexchange:PublishDataSet redshift:AuthorizeDataShare
TagResource	Concede permissão para adicionar uma ou mais etiquetas a um recurso especificado	Marcação	data-grants		
			data-sets		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			event-actions		
			revisions		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover uma ou mais etiquetas de um recurso especificado	Tags	data-grants		
			data-sets		
			event-actions		
			revisions		
				aws:TagKeys	
UpdateAsset	Concede permissão para obter informações de atualização sobre um ativo	Gravar	assets*		
UpdateDataSet	Concede permissão para atualizar informações sobre um conjunto de dados	Gravar	data-sets*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateEventAction	Concede permissão para atualizar informações para uma ação de evento	Gravar	event-actions*		
UpdateRevision	Concede permissão para atualizar informações sobre uma revisão	Gravar	revisions*		dataexchange:PublishDataSet dataexchange:PublishToDataGrant

Tipos de recursos definidos pelo AWS Data Exchange

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
jobs	`arn:${Partition}:dataexchange:${Region}:${Account}:jobs/${JobId}`	dataexchange:JobType
data-sets	`arn:${Partition}:dataexchange:${Region}:${Account}:data-sets/${DataSetId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
entitled-data-sets	`arn:${Partition}:dataexchange:${Region}::data-sets/${DataSetId}`	
revisions	`arn:${Partition}:dataexchange:${Region}:${Account}:data-sets/${DataSetId}/revisions/${RevisionId}`	aws:ResourceTag/${TagKey}
entitled-revisions	`arn:${Partition}:dataexchange:${Region}::data-sets/${DataSetId}/revisions/${RevisionId}`	
assets	`arn:${Partition}:dataexchange:${Region}:${Account}:data-sets/${DataSetId}/revisions/${RevisionId}/assets/${AssetId}`	
entitled-assets	`arn:${Partition}:dataexchange:${Region}::data-sets/${DataSetId}/revisions/${RevisionId}/assets/${AssetId}`	
event-actions	`arn:${Partition}:dataexchange:${Region}:${Account}:event-actions/${EventActionId}`	aws:ResourceTag/${TagKey}
data-grants	`arn:${Partition}:dataexchange:${Region}:${Account}:data-grants/${DataGrantId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Data Exchange

AWS O Data Exchange define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelo conjunto de valores permitidos para cada uma das etiquetas obrigatórias na solicitação de criação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelo valor de etiqueta associado ao recurso	String
aws:TagKeys	Filtra o acesso pela presença de etiquetas obrigatórias na solicitação de criação	ArrayOfString
dataexchange:JobType	Filtra o acesso pelo tipo de trabalho especificado	String

Ações, recursos e chaves de condição do Amazon Data Lifecycle Manager

O Amazon Data Lifecycle Manager (prefixo do serviço: `dlm`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Data Lifecycle Manager
- Tipos de recursos definidos pelo Amazon Data Lifecycle Manager
- Chaves de condição do Amazon Data Lifecycle Manager

Ações definidas pelo Amazon Data Lifecycle Manager

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateLifecyclePolicy	Concede permissão para criar uma política de ciclo de vida de dados para gerenciar a criação e a retenção programadas de snapshots do Amazon EBS. Você pode ter até 100 políticas	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteLifecyclePolicy	Concede permissão para excluir uma política de ciclo de vida de dados existente. Além disso, essa ação interrompe a criação e a exclusão de snapshots especificadas pela política. Os snapshots existentes não são afetados	Gravar	policy*		
GetLifecyclePolicies	Concede permissão para retornar uma lista de descrições de resumo de políticas de ciclo de vida de dados	Lista			
GetLifecyclePolicy	Concede permissão para retornar uma descrição completa de uma única política de ciclo de vida de dados	Leitura	policy*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar as etiquetas associadas a um recurso	Leitura	policy*		
TagResource	Concede permissão para adicionar ou atualizar as etiquetas de um recurso	Tags	policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover etiquetas associadas a um recurso	Tags	policy*		
				aws:TagKeys	
UpdateLifecyclePolicy	Concede permissão para atualizar uma política de ciclo de vida de dados existente	Gravar	policy*		

Tipos de recursos definidos pelo Amazon Data Lifecycle Manager

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
policy	`arn:${Partition}:dlm:${Region}:${Account}:policy/${ResourceName}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Data Lifecycle Manager

O Amazon Data Lifecycle Manager define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Data Pipeline

AWS O Data Pipeline (prefixo do serviço:`datapipeline`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.

- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Data Pipeline
- Tipos de recursos definidos pelo AWS Data Pipeline
- Chaves de condição do AWS Data Pipeline

Ações definidas pelo AWS Data Pipeline

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ActivatePipeline	Concede permissão para validar o pipeline especificado e inicia as tarefas de processamento do pipeline. Se o pipeline não passar na validação, a ativação falhará	Gravar	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} datapipeline:workerGroup	
AddTags	Concede permissão para adicionar ou modificar etiquetas do pipeline especificado	Tags	pipeline*		
				datapipeline:PipelineCreator	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				datapipeline:Tag/${TagKey} aws:TagKeys aws:RequestTag/${TagKey}	
CreatePipeline	Concede permissão para criar um novo pipeline vazio	Gravar		aws:RequestTag/${TagKey} aws:TagKeys datapipeline:Tag/${TagKey}	datapipeline:AddTags
DeactivatePipeline	Concede permissão para desativar o pipeline em execução especificado	Gravar	pipeline*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} datapipeline:workerGroup	
DeletePipeline	Concede permissão para excluir um pipeline, a definição do pipeline e o histórico de execuções	Gravar	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	
DescribeObjects	Concede permissão para obter as definições de objetos de um conjunto de objetos associados ao pipeline	Leitura	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribePipelines	Concede permissão para recuperar metadados sobre um ou mais pipelines	Leitura	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	
EvaluateExpression	Concede permissão aos executores de tarefas para chamar EvaluateExpression e avaliar uma string no contexto do objeto especificado	Leitura	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	
GetAccountLimits [somente permissão]	Concede permissão para ligar GetAccountLimits	Lista			
GetPipelineDefinition	Concede permissão para obter a definição do pipeline especificado	Leitura	pipeline*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} datapipeline:workerGroup	
ListPipelines	Concede permissão para listar os identificadores de pipeline de todos os pipelines ativos que você tem permissão para acessar	Lista			
PollForTask	Concede permissão aos executores de tarefas para chamar PollForTask e receber uma tarefa a ser executada do AWS Data Pipeline	Gravar		datapipeline:workerGroup	
PutAccountLimits [somente permissão]	Concede permissão para ligar PutAccountLimits	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutPipelineDefinition	Concede permissão para adicionar tarefas, programações e pré-condições ao pipeline especificado	Gravar	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} datapipeline:workerGroup	
QueryObjects	Concede permissão para consultar o pipeline para obter os nomes de objetos que correspondem ao conjunto de condições especificadas	Leitura	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RemoveTags	Concede permissão para remover as etiquetas da fila do SQS para o pipeline especificado	Tags	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} aws:TagKeys aws:RequestTag/${TagKey}	
ReportTaskProgress	Concede permissão aos executores de tarefas para chamarem ReportTaskProgress, quando recebem uma tarefa, para reconhecer que ela tem a tarefa	Gravar	pipeline*		
ReportTaskRunnerHeartbeat	Concede permissão aos executores de tarefas para ligar a ReportTaskRunnerHeartbeat cada 15 minutos para indicar que estão operacionais	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SetStatus	Concede permissão para solicitar que o status dos objetos físicos ou lógicos especificados do pipeline sejam atualizados no pipeline especificado	Gravar	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	
SetTaskStatus	Concede permissão aos executores de tarefas para ligar SetTaskStatus para notificar o AWS Data Pipeline de que uma tarefa foi concluída e fornecer informações sobre o status final	Gravar	pipeline*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ValidatePipelineDefinition	Concede permissão para validar a definição do pipeline especificado para garantir que está bem formado e pode ser executado sem erros	Leitura	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} datapipeline:workerGroup	

Tipos de recursos definidos pelo AWS Data Pipeline

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
pipeline	`arn:${Partition}:datapipeline:${Region}:${Account}:pipeline/${PipelineId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Data Pipeline

AWS O Data Pipeline define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString
datapipeline:PipelineCreator	Filtra acesso pelo usuário do IAM que criou o pipeline	ArrayOfString
datapipeline:Tag/${TagKey}	Filtra o acesso por key/value par especificado pelo cliente que pode ser anexado a um recurso	String
datapipeline:workerGroup	Filtra o acesso pelo nome do grupo de operadores para o qual um executor de tarefas recupera o trabalho	ArrayOfString

Ações, recursos e chaves de condição do AWS Database Migration Service

AWS O Database Migration Service (prefixo do serviço:`dms`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Database Migration Service
- Tipos de recursos definidos pelo AWS Database Migration Service
- Chaves de condição do AWS Database Migration Service

Ações definidas pelo AWS Database Migration Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddTagsToResource	Concede permissão para adicionar etiquetas de metadados a recursos DMS, incluindo instâncias de replicação, endpoints, grupos de segurança e tarefas de migração	Marcação	Certificate		
			DataMigration		
			DataProvider		
			Endpoint		
			EventSubscription		
			InstanceProfile		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			MigrationProject		
			ReplicationConfig		
			ReplicationInstance		
			ReplicationSubnetGroup		
			ReplicationTask		
			ReplicationTaskAssessmentRun		
			ReplicationTaskIndividualAssessment		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
ApplyPendingMaintenanceAction	Concede permissão para aplicar uma ação de manutenção pendente a um recurso (por exemplo, a uma instância de replicação)	Gravar	ReplicationInstance*		
AssociateExtensionPack	Concede permissão para associar um pacote de extensão	Gravar	MigrationProject*		
BatchStartRecommendations	Concede permissão para iniciar a análise de até 20 bancos de dados de origem para recomendar mecanismos de destino a cada banco de dados de origem	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelReplicationTaskAssessmentRun	Concede permissão para cancelar uma única execução de avaliação de pré-migração	Gravar	ReplicationTaskAssessmentRun*		
CreateDataMigration	Concede permissão para criar uma migração de banco de dados usando as configurações fornecidas	Gravar	MigrationProject*		iam:PassRole
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDataProvider	Concede permissão para criar um provedor de dados usando as configurações fornecidas	Gravar		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole
CreateEndpoint	Concede permissão para criar um endpoint usando as configurações fornecidas	Gravar		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateEventSubscription	Concede permissão para criar uma assinatura de notificação de eventos do AWS DMS	Gravar		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
CreateFleetAdvisorCollector	Concede permissão para criar um coletor do Fleet Advisor usando os parâmetros especificados	Gravar			iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateInstanceProfile	Concede permissão para criar um perfil de instância usando as configurações fornecidas	Gravar		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole
CreateMigrationProject	Concede permissão para criar um projeto de migração usando as configurações fornecidas	Gravar	DataProvider* InstanceProfile*		iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
CreateReplicationConfig	Concede permissão para criar uma configuração de replicação usando as configurações fornecidas	Gravar	Endpoint*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateReplicationInstance	Concede permissão para criar uma instância de replicação usando os parâmetros especificados	Gravar		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole
CreateReplicationSubnetGroup	Concede permissão para criar um grupo de sub-redes de replicação com uma lista da sub-rede IDs em uma VPC	Gravar		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateReplicationTask	Concede permissão para criar uma tarefa de replicação usando os parâmetros especificados	Gravação	Endpoint*		
			ReplicationInstance*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
DeleteCertificate	Concede permissão para excluir o certificado especificado	Gravação	Certificate*		
DeleteConnection	Concede permissão para excluir a conexão especificada entre uma instância de replicação e um endpoint.	Gravar	Endpoint*		
			ReplicationInstance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteDataMigration	Concede permissão para excluir a migração de banco de dados especificada	Gravar	DataMigration*		
DeleteDataProvider	Concede permissão para excluir o provedor de dados especificado	Gravar	DataProvider*		
DeleteEndpoint	Concede permissão para excluir o endpoint especificado	Gravar	Endpoint*		
DeleteEventSubscription	Concede permissão para excluir uma assinatura de evento do AWS DMS	Gravar	EventSubscription*		
DeleteFleetAdvisorCollector	Concede permissão para excluir o coletor especificado do Fleet Advisor	Gravar			
DeleteFleetAdvisorDatabases	Concede permissão para excluir os bancos de dados especificados do Fleet Advisor	Gravar			
DeleteInstanceProfile	Concede permissão para excluir o perfil de instância especificado	Gravar	InstanceProfile*		
DeleteMigrationProject	Concede permissão para excluir o projeto de migração especificado	Gravar	MigrationProject*		
DeleteReplicationConfig	Concede permissão para excluir a configuração de replicação especificada	Gravar	ReplicationConfig*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteReplicationInstance	Concede permissão para excluir a instância de replicação especificada	Gravação	ReplicationInstance*		
DeleteReplicationSubnetGroup	Concede permissão para excluir um grupo de sub-redes	Gravação	ReplicationSubnetGroup*		
DeleteReplicationTask	Concede permissão para excluir a tarefa de replicação especificada	Gravação	ReplicationTask*		
DeleteReplicationTaskAssessmentRun	Concede permissão para excluir o registro de uma única execução de avaliação de pré-migração	Gravar	ReplicationTaskAssessmentRun*		
DescribeAccountAttributes	Concede permissão para listar todos os atributos do AWS DMS para uma conta de cliente	Leitura			
DescribeApplicableIndividualAssessments	Concede permissão para listar avaliações individuais que você pode especificar para uma nova execução de avaliação de pré-migração	Leitura	ReplicationInstance		
			ReplicationTask		
DescribeCertificates	Concede permissão para fornecer uma descrição do certificado	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeConnections	Concede permissão para descrever o status das conexões que foram feitas entre a instância de replicação e um endpoint	Leitura			
DescribeConversionConfiguration	Concede permissão para retornar informações sobre a configuração do projeto do DMS Schema Conversion	Leitura	MigrationProject*		
DescribeDataMigrations	Concede permissão para retornar informações sobre migrações de banco de dados para sua conta na região especificada	Leitura			
DescribeEndpointSettings	Concede permissão para retornar as possíveis configurações de endpoint disponíveis quando você cria um endpoint para um mecanismo de banco de dados específico	Leitura			
DescribeEndpointTypes	Concede permissão para retornar informações sobre o tipo de endpoints disponíveis	Leitura			
DescribeEndpoints	Concede permissão para retornar informações sobre os endpoints da sua conta na região atual	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeEngineVersions	Concede permissão para retornar informações sobre as versões disponíveis para instâncias de replicação do DMS	Leitura			
DescribeEventCategories	Concede permissão para listar categorias para todos os tipos de origem de eventos ou, se especificado, para um tipo de origem especificado	Leitura			
DescribeEventSubscriptions	Concede permissão para listar todas as assinaturas de eventos de uma conta de cliente	Leitura			
DescribeEvents	Concede permissão para listar eventos para um determinado identificador de origem e tipo de origem	Leitura			
DescribeFleetAdvisorCollectors	Concede permissão para retornar uma lista paginada de coletores do Fleet Advisor em sua conta com base nas configurações de filtro	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeFleetAdvisorDatabases	Concede permissão para retornar uma lista paginada de bancos de dados do Fleet Advisor em sua conta com base nas configurações de filtro	Leitura			
DescribeFleetAdvisorLsaAnalysis	Concede permissão para retornar uma lista paginada de descrições de análises de Large-Scale Assessment (LSA – Avaliação em grande escala) produzidas por seus coletores do Fleet Advisor	Leitura			
DescribeFleetAdvisorSchemaObjectSummary	Concede permissão para retornar uma lista paginada de descrições de esquemas descobertos por seus coletores do Fleet Advisor com base nas configurações de filtro	Leitura			
DescribeFleetAdvisorSchemas	Concede permissão para retornar uma lista paginada de esquemas descobertos por seus coletores do Fleet Advisor com base nas configurações de filtro	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeMetadataModelImports	Concede permissão para retornar informações sobre o início das operações de importação do modelo de metadados para um projeto de migração	Leitura	Migration Project*		
DescribeOrderableReplicationInstances	Concede permissão para retornar informações sobre os tipos de instância de replicação que podem ser criados na região especificada	Leitura			
DescribePendingMaintenanceActions	Concede permissão para retornar informações sobre ações de manutenção pendentes	Leitura			
DescribeRecommendationLimitations	Concede permissão para retornar uma lista paginada de descrições de limitações para recomendações de mecanismos de destino AWS	Leitura			
DescribeRecommendations	Concede permissão para retornar uma lista paginada de descrições de recomendações de mecanismos de destino para seus bancos de dados de origem	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeRefreshSchemasStatus	Concede permissão para retornar o status da RefreshSchemas operação	Leitura	Endpoint*		
DescribeReplicationConfigs	Concede permissão para descrever configurações de replicação	Leitura			
DescribeReplicationInstanceTaskLogs	Concede permissão para retornar informações sobre os logs de tarefas para a tarefa especificada	Leitura	ReplicationInstance*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
DescribeReplicationInstances	Concede permissão para retornar informações sobre instâncias de replicação para sua conta na região atual	Leitura			
DescribeReplicationSubnetGroups	Concede permissão para retornar informações sobre os grupos de sub-redes de replicação	Leitura			
DescribeReplicationTableStatistics	Concede permissão para descrever as estatísticas da tabela de replicação	Leitura	ReplicationConfig*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeReplicationTaskAssessmentResults	Concede permissão para retornar os resultados mais recentes da avaliação de tarefas do Amazon S3	Leitura	ReplicationTask		
DescribeReplicationTaskAssessmentRuns	Concede permissão para retornar uma lista paginada de execuções de avaliação de pré-migração com base nas configurações de filtro	Leitura	ReplicationInstance		
			ReplicationTask		
			ReplicationTaskAssessmentRun		
DescribeReplicationTaskIndividualAssessments	Concede permissão para retornar uma lista paginada de avaliações individuais com base nas configurações de filtro	Leitura	ReplicationTask		
			ReplicationTaskAssessmentRun		
DescribeReplicationTasks	Concede permissão para retornar informações sobre tarefas de replicação para sua conta na região atual	Leitura			
DescribeReplications	Concede permissão para descrever replicações	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeSchemas	Concede permissão para retornar informações sobre o esquema para o endpoint especificado	Leitura	Endpoint*		
DescribeTableStatistics	Concede permissão para retornar estatísticas de tabela na tarefa de migração do banco de dados, incluindo nome da tabela, linhas inseridas, linhas atualizadas e linhas excluídas	Leitura	ReplicationTask*		
ExportMetadataModelAssessment	Concede permissão para exportar a avaliação do modelo de metadados especificado	Gravar	MigrationProject		
ImportCertificate	Concede permissão para enviar o certificado especificado	Gravar		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
ListDataProviders	Concede permissão para listar os atributos do AWS DMS para um provedor de dados	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListExtensionPacks	Concede permissão para listar os atributos do AWS DMS para um pacote de extensão	Leitura	MigrationProject		
ListInstanceProfiles	Concede permissão para listar os atributos do AWS DMS para os perfis de uma instância	Leitura	InstanceProfile		
ListMetadataModelAssessmentActionItems [somente permissão]	Concede permissão para listar os atributos do AWS DMS para os itens de ação de avaliação de um modelo de metadados. Observação. Apesar dessa ação ser necessária StartMetadataModelImport, esta última não autoriza atualmente a operação de conversão de esquema descrita.	Leitura	MigrationProject		dms:StartMetadataModelImport
ListMetadataModelAssessments	Concede permissão para listar os atributos do AWS DMS para as avaliações de um modelo de metadados	Leitura	MigrationProject		
ListMetadataModelConversions	Concede permissão para listar os atributos do AWS DMS para as conversões de um modelo de metadados	Leitura	MigrationProject		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListMetadataModelExports	Concede permissão para listar os atributos do AWS DMS para as exportações de um modelo de metadados	Leitura	MigrationProject		
ListMigrationProjects	Concede permissão para listar os atributos do AWS DMS para um projeto de migração. Observação. Apesar dessa ação exigir DescribeMigrationProjects e DescribeConversionConfiguration, ambas as ações necessárias não autorizam atualmente a operação de conversão de esquema descrita.	Leitura	DataProvider		dms:DescribeConversionConfiguration
			InstanceProfile		
			MigrationProject		
ListTagsForResource	Concede permissão para listar todas as tags de um AWS recurso DMS	Leitura	Certificate		
			DataMigration		
			DataProvider		
			Endpoint		
			EventSubscription		
			InstanceProfile		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			Migration Project		
			ReplicationConfig		
			ReplicationInstance		
			ReplicationSubnetGroup		
			ReplicationTask		
			ReplicationTaskAssessmentRun		
			ReplicationTaskIndividualAssessment		
ModifyDataMigration	Concede permissão para modificar a migração de banco de dados especificada	Gravar	DataMigration*		iam:PassRole
ModifyEndpoint	Concede permissão para modificar o endpoint especificado	Gravar	Endpoint*		iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			Certificate		
ModifyEventSubscription	Concede permissão para modificar uma assinatura existente de notificação de eventos do AWS DMS	Gravar			
ModifyFleetAdvisorCollector [somente permissão]	Concede permissão para modificar o nome e a descrição do coletor especificado do Fleet Advisor	Gravar			
ModifyFleetAdvisorCollectorStatuses [somente permissão]	Concede permissão para modificar o status do coletor especificado do Fleet Advisor	Gravar			
ModifyReplicationConfig	Concede permissão para modificar a configuração de replicação especificada	Gravar	ReplicationConfig*		
ModifyReplicationInstance	Concede permissão para modificar a instância de replicação para aplicar novas configurações	Gravação	ReplicationInstance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ModifyReplicationSubnetGroup	Concede permissão para modificar as configurações do grupo de sub-redes de replicação especificado	Gravação			
ModifyReplicationTask	Concede permissão para modificar a tarefa de replicação especificada	Gravação	ReplicationTask*		
MoveReplicationTask	Concede permissão para transferir a tarefa de replicação especificada para outra instância de replicação.	Gravação	ReplicationInstance*		
			ReplicationTask*		
RebootReplicationInstance	Concede permissão para reiniciar uma instância de replicação. A reinicialização resulta em uma interrupção momentânea, até que a instância de replicação fique disponível novamente	Gravação	ReplicationInstance*		
RefreshSchemas	Concede permissão para preencher o esquema para o endpoint especificado	Gravar	Endpoint*		
			ReplicationInstance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ReloadReplicationTables	Concede permissão para recarregar a tabela de banco de dados de destino com a origem para uma replicação	Gravar	ReplicationConfig*		
ReloadTables	Concede permissão para recarregar a tabela do banco de dados de destino com os dados de origem	Gravação	ReplicationTask*		
RemoveTagsFromResource	Concede permissão para remover etiquetas de metadados de um recurso DMS	Tags	Certificate		
			DataMigration		
			DataProvider		
			Endpoint		
			EventSubscription		
			InstanceProfile		
			MigrationProject		
			ReplicationConfig		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			ReplicationInstance		
			ReplicationSubnetGroup		
			ReplicationTask		
			ReplicationTaskAssessmentRun		
			ReplicationTaskIndividualAssessment		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RunFleetAdvisorLsaAnalysis	Concede permissão para executar uma análise de avaliação em grande escala (LSA) em cada coletor do Fleet Advisor em sua conta	Gravar			
StartDataMigration	Concede permissão para iniciar a migração de banco de dados	Gravar	DataMigration*		
StartMetadataModelAssessment	Concede permissão para iniciar uma nova avaliação de modelo de metadados	Gravar	MigrationProject*		
StartMetadataModelConversion	Concede permissão para iniciar uma nova conversão de modelo de metadados	Gravar	MigrationProject*		
StartMetadataModelExportAsScripts	Concede permissão para iniciar uma nova exportação de modelo de metadados como script	Gravar	MigrationProject*		
StartMetadataModelExportToTarget	Concede permissão para iniciar uma nova exportação de modelo de metadados para destino	Gravar	MigrationProject*		
StartMetadataModelImport	Concede permissão para iniciar uma nova importação de modelo de metadados	Gravar	MigrationProject*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartRecommendations	Concede permissão para iniciar a análise de banco de dados de origem para fornecer recomendações de mecanismos de destino	Gravar			
StartReplication	Concede permissão para iniciar uma replicação	Gravar	ReplicationConfig*		
StartReplicationTask	Concede permissão para iniciar a tarefa de replicação	Gravação	ReplicationTask*		
StartReplicationTaskAssessment	Concede permissão para iniciar a avaliação da tarefa de replicação para tipos de dados não suportados no banco de dados de origem	Gravação	ReplicationTask*		
StartReplicationTaskAssessmentRun	Concede permissão para iniciar uma nova avaliação de pré-migração para uma ou mais avaliações individuais de uma tarefa de migração	Gravar	ReplicationTask*		iam:PassRole
StopDataMigration	Concede permissão para parar a migração de banco de dados	Gravar	DataMigration*		
StopReplication	Concede permissão para interromper uma replicação	Gravar	ReplicationConfig*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopReplicationTask	Concede permissão para interromper a tarefa de replicação	Gravação	ReplicationTask*		
TestConnection	Concede permissão para testar a conexão entre a instância de replicação e o endpoint	Leitura	Endpoint*		
			ReplicationInstance*		
UpdateConversionConfiguration	Concede permissão para atualizar uma configuração de conversão	Gravar	MigrationProject*		
UpdateDataProvider	Concede permissão para atualizar o provedor de dados especificado	Gravar	DataProvider*		
UpdateInstanceProfile	Concede permissão para atualizar o perfil de instância especificado	Gravar	InstanceProfile*		
UpdateMigrationProject	Concede permissão para atualizar o projeto de migração especificado	Gravar	MigrationProject*		
UpdateSubscriptionsToEventBridge	Concede permissão para migrar assinaturas de DMS para o Eventbridge	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UploadFileMetadataList [somente permissão]	Concede permissão para carregar arquivos para seu bucket do Amazon S3.	Gravar			

Tipos de recursos definidos pelo AWS Database Migration Service

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Tipos de recursos	ARN	Chaves de condição
		dms:data-migration-tag/${TagKey}
Endpoint	arn:${Partition}:dms:${Region}:${Account}:endpoint:*	aws:ResourceTag/${TagKey} dms:endpoint-tag/${TagKey}
EventSubscription	arn:${Partition}:dms:${Region}:${Account}:es:*	aws:ResourceTag/${TagKey} dms:es-tag/${TagKey}
InstanceProfile	arn:${Partition}:dms:${Region}:${Account}:instance-profile:*	aws:ResourceTag/${TagKey} dms:instance-profile-tag/${TagKey}
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}

Tipos de recursos	ARN	Chaves de condição
ReplicationSubnetGroup	`arn:${Partition}:dms:${Region}:${Account}:subgrp:*`	aws:ResourceTag/${TagKey} dms:subgrp-tag/${TagKey}
ReplicationTask	`arn:${Partition}:dms:${Region}:${Account}:task:*`	aws:ResourceTag/${TagKey} dms:task-tag/${TagKey}
ReplicationTaskAssessmentRun	`arn:${Partition}:dms:${Region}:${Account}:assessment-run:*`	aws:ResourceTag/${TagKey} dms:assessment-run-tag/${TagKey}
ReplicationTaskIndividualAssessment	`arn:${Partition}:dms:${Region}:${Account}:individual-assessment:*`	aws:ResourceTag/${TagKey} dms:individual-assessment-tag/${TagKey}

Chaves de condição do AWS Database Migration Service

AWS O Database Migration Service define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pela presença de pares chave-valor da etiqueta anexados ao recurso	Segmento
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString
dms:assessment-run-tag/${TagKey}	Filtra o acesso pela presença de pares de chave-valor de tag na solicitação de AssessmentRun	String
dms:cert-tag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação para Certificate (Certificado)	String
dms:data-migration-tag/${TagKey}	Filtra o acesso pela presença de pares de chave-valor de tag na solicitação de DataMigration	String
dms:data-provider-tag/${TagKey}	Filtra o acesso pela presença de pares de chave-valor de tag na solicitação de DataProvider	String
dms:endpoint-tag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação para Endpoint	String
dms:es-tag/${TagKey}	Filtra o acesso pela presença de pares de chave-valor de tag na solicitação de EventSubscription	String
dms:individual-assessment-tag/${TagKey}	Filtra o acesso pela presença de pares de chave-valor de tag na solicitação de IndividualAssessment	String

Chaves de condição	Descrição	Tipo
dms:instance-profile-tag/${TagKey}	Filtra o acesso pela presença de pares de chave-valor de tag na solicitação de InstanceProfile	String
dms:migration-project-tag/${TagKey}	Filtra o acesso pela presença de pares de chave-valor de tag na solicitação de MigrationProject	String
dms:rep-tag/${TagKey}	Filtra o acesso pela presença de pares de chave-valor de tag na solicitação de ReplicationInstance	String
dms:replication-config-tag/${TagKey}	Filtra o acesso pela presença de pares de chave-valor de tag na solicitação de ReplicationConfig	String
dms:req-tag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação fornecida	String
dms:subgrp-tag/${TagKey}	Filtra o acesso pela presença de pares de chave-valor de tag na solicitação de ReplicationSubnetGroup	String
dms:task-tag/${TagKey}	Filtra o acesso pela presença de pares de chave-valor de tag na solicitação de ReplicationTask	String

Ações, recursos e chaves de condição do Database Query Metadata Service

O Database Query Metadata Service (prefixo do serviço: `dbqms`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.

- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Database Query Metadata Service
- Tipos de recursos definidos pelo Database Query Metadata Service
- Chaves de condição do Database Query Metadata Service

Ações definidas pelo Database Query Metadata Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateFavoriteQuery	Concede permissão para criar uma consulta favorita	Write			
CreateQueryHistory	Concede permissão para adicionar uma consulta ao histórico	Write			
CreateTab	Concede permissão para criar uma guia de consulta	Write			
DeleteFavoriteQueries	Concede permissão para excluir consultas salvas	Write			
DeleteQueryHistory	Concede permissão para excluir uma consulta histórica	Write			
DeleteTab	Concede permissão para excluir guia de consulta	Write			
DescribeFavoriteQueries	Concede permissão para listar consultas salvas e metadados associados	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeQueryHistory	Concede permissão para listar o histórico de consultas executadas	List			
DescribeTabs	Concede permissão para listar guias de consulta e metadados associados	List			
GetQueryString	Concede permissão para recuperar string de consulta favorita ou histórico por ID	Read			
UpdateFavoriteQuery	Concede permissão para atualizar a consulta e a descrição salvas	Write			
UpdateQueryHistory	Concede permissão para atualizar o histórico de consultas	Write			
UpdateTab	Concede permissão para atualizar a guia de consulta	Write			

Tipos de recursos definidos pelo Database Query Metadata Service

O Database Query Metadata Service não oferece suporte à especificação de um ARN de recurso no elemento `Resource` de uma declaração de política do IAM. Para permitir o acesso ao Database Query Metadata Service, especifique `"Resource": "*"` em sua política.

Chaves de condição do Database Query Metadata Service

O DBQMS não tem chaves de contexto específicas ao serviço que possam ser usadas no elemento `Condition` de uma declaração de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o AWS DataSync

AWS DataSync (prefixo do serviço:`datasync`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS DataSync
- Tipos de recursos definidos pelo AWS DataSync
- Chaves de condição do AWS DataSync

Ações definidas pelo AWS DataSync

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos

("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddStorageSystem	Concede permissão para criar um sistema de armazenamento	Gravar	agent*		
				aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:TagKeys	
CancelTaskExecution	Concede permissão para cancelar a execução de uma tarefa de sincronização	Write	taskexecution*		
				aws:ResourceTag/${TagKey}	
CreateAgent	Concede permissão para ativar um agente que você implantou em seu host	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationAzureBlob	Concede permissão para criar um endpoint para um contêiner do Microsoft Azure Blob Storage	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationEfs	Concede permissão para criar um endpoint para um sistema de arquivos do Amazon EFS	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateLocationFsxLustre	Concede permissão para criar um endpoint para um Amazon FSx Lustre	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationFsxOntap	Concede permissão para criar um endpoint para a Amazon FSx for ONTAP	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationFsxOpenZfs	Concede permissão para criar um endpoint para Amazon FSx for OpenZFS	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationFsxWindows	Concede permissão para criar um endpoint para um sistema de arquivos FSx do Amazon Windows File Server	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationHdfs	Concede permissão para criar um endpoint para um Amazon Hdfs	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateLocationNfs	Concede permissão para criar um endpoint para um sistema de arquivos NFS	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationObjectStorage	Concede permissão para criar um endpoint para um bucket de armazenamento de objetos autogerenciado	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationS3	Concede permissão para criar um endpoint para um bucket do Amazon S3	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationSmb	Concede permissão para criar um endpoint para um sistema de arquivos SMB	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTask	Concede permissão para criar uma tarefa de sincronização	Gravar	location* agent		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAgent	Concede permissão para excluir um agente	Gravar	agent*		
DeleteLocation	Concede permissão para excluir um local usado por AWS DataSync	Gravar	location*		
DeleteTask	Concede permissão para excluir uma tarefa de sincronização	Write	task*		
DescribeAgent	Concede permissão para visualizar metadados, como nome, interfaces de rede e status (ou seja, se o agente está em execução ou não) sobre um agente de sincronização	Leitura	agent*		
DescribeDiscoveryJob	Concede permissão para descrever metadados sobre um trabalho de descoberta	Leitura	discoveryjob*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeLocationAzureBlob	Concede permissão para exibir metadados, como informações de caminho, sobre um local de sincronização do Azure Blob Storage	Leitura	location*		
DescribeLocationEfs	Concede permissão para exibir metadados, como informações de caminho sobre um local de sincronização do Amazon EFS	Leitura	location*		
DescribeLocationFsxLustre	Concede permissão para visualizar metadados, como as informações do caminho sobre um local de sincronização do Amazon FSx Lustre	Leitura	location*		
DescribeLocationFsxOntap	Concede permissão para visualizar metadados, como as informações do caminho sobre um local de sincronização do Amazon FSx for ONTAP	Leitura	location*		
DescribeLocationFsxOpenZfs	Concede permissão para visualizar metadados, como as informações do caminho sobre um local de sincronização do Amazon FSx OpenZFS	Leitura	location*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeLocationFsxWindows	Concede permissão para visualizar metadados, como as informações do caminho sobre um local de sincronização FSx do Amazon Windows	Leitura	location*		
DescribeLocationHdfs	Concede permissão para exibir metadados, como informações de caminho sobre um local de sincronização do Amazon HDFS	Leitura	location*		
DescribeLocationNfs	Concede permissão para exibir metadados, como informações de caminho, sobre um local de sincronização NFS	Read	location*		
DescribeLocationObjectStorage	Concede permissão para exibir metadados sobre um local de servidor de armazenamento de objetos autogerenciado	Read	location*		
DescribeLocationS3	Concede permissão para exibir metadados, como nome do bucket, sobre um local de sincronização de bucket do Amazon S3	Read	location*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeLocationSmb	Concede permissão para exibir metadados, como informações de caminho, sobre um local de sincronização SMB	Leitura	location*		
DescribeStorageSystem	Concede permissão para visualizar metadados sobre um sistema de armazenamento	Leitura	storagesystem*		
DescribeStorageSystemResourceMetrics	Concede permissão para descrever as métricas de recursos coletadas por um trabalho de descoberta	Lista	discoveryjob*		
DescribeStorageSystemResources	Concede permissão para descrever recursos identificados por um trabalho de descoberta	Lista	discoveryjob*		
DescribeTask	Concede permissão para exibir metadados sobre uma tarefa de sincronização	Read	task*		
DescribeTaskExecution	Concede permissão para exibir metadados sobre uma tarefa de sincronização que está sendo executada	Leitura	taskexecution*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GenerateRecommendations	Concede permissão para gerar recomendações para um recurso identificado por um trabalho de descoberta	Gravar	discoveryjob*		
ListAgents	Concede permissão para listar agentes pertencentes a um Conta da AWS em uma região especificada na solicitação	Lista			
ListDiscoveryJobs	Concede permissão para listar trabalhos de descoberta	Lista			
ListLocations	Concede permissão para listar locais de sincronização de origem e destino	Lista			
ListStorageSystems	Concede permissão para listar sistemas de armazenamento	Lista			
ListTagsForResource	Concede permissão para listar etiquetas que foram adicionadas ao recurso especificado	Read	agent		
			discoveryjob		
			location		
			storagesystem		
			task		
			taskexecution		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTaskExecutions	Concede permissão para listar tarefas de sincronização executadas	List		aws:ResourceTag/${TagKey}	
ListTasks	Concede permissão para listar todas as tarefas de sincronização	Lista			
RemoveStorageSystem	Concede permissão para excluir um sistema de armazenamento	Gravar	storagesystem*		
StartDiscoveryJob	Concede permissão para iniciar um trabalho de descoberta para um sistema de armazenamento	Gravar	storagesystem*		
StartTaskExecution	Concede permissão para iniciar uma invocação específica de uma tarefa de sincronização	Gravar	task*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
StopDiscoveryJob	Concede permissão para interromper um trabalho de descoberta	Gravar	discoveryjob*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para aplicar um par de valores-chave a um recurso AWS	Tags	agent		
			discoveryjob		
			location		
			storagesystem		
			task		
			taskexecution		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover uma ou mais etiquetas do recurso especificado	Tags	agent		
			discoveryjob		
			location		
			storagesystem		
			task		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			taskexecution		
				aws:TagKeys	
UpdateAgent	Concede permissão para atualizar o nome de um atendente	Gravar	agent*		
UpdateDiscoveryJob	Concede permissão para atualizar um trabalho de descoberta	Gravar	discoveryjob*		
UpdateLocationAzureBlob	Concede permissão para atualizar um local de sincronização do Azure Blob Storage	Gravar	location*		
UpdateLocationEfs	Concede permissão para atualizar um local de sincronização do EFS	Gravar	location*		
UpdateLocationFsxLustre	Concede permissão para atualizar um local de sincronização do FSx Lustre	Gravar	location*		
UpdateLocationFsxOntap	Concede permissão para atualizar um local de sincronização do FSx ONTAP	Gravar	location*		
UpdateLocationFsxOpenZfs	Concede permissão para atualizar um local de FSx sincronização do OpenZFS	Gravar	location*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateLocationFsxWindows	Concede permissão para atualizar um local de sincronização FSx do Windows	Gravar	location*		
UpdateLocationHdfs	Concede permissão para atualizar um local de sincronização do HDFS	Gravar	location*		
UpdateLocationNfs	Concede permissão para atualizar um local de sincronização do NFS	Write	location*		
UpdateLocationObjectStorage	Concede permissão para atualizar um local de servidor de armazenamento de objetos autogerenciado	Gravar	location*		
UpdateLocationS3	Concede permissão para atualizar um local de sincronização do S3	Gravar	location*		
UpdateLocationSmb	Concede permissão para atualizar um local de sincronização do SMB	Gravar	location*		
UpdateStorageSystem	Concede permissão para atualizar um sistema de armazenamento	Gravar	storagesystem*		
UpdateTask	Concede permissão para atualizar metadados associados a uma tarefa de sincronização	Write	task*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateTaskExecution	Concede permissão para atualizar a execução de uma tarefa de sincronização	Gravar	taskexecution*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pelo AWS DataSync

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Tipos de recursos	ARN	Chaves de condição
storagesystem	`arn:${Partition}:datasync:${Region}:${AccountId}:system/${StorageSystemId}`	aws:ResourceTag/${TagKey}
discoveryjob	`arn:${Partition}:datasync:${Region}:${AccountId}:system/${StorageSystemId}/job/${DiscoveryJobId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS DataSync

AWS DataSync define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso pelos pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelos pares chave-valor de etiqueta associados ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para a Amazon DataZone

A Amazon DataZone (prefixo do serviço:`datazone`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon DataZone
- Tipos de recursos definidos pela Amazon DataZone
- Chaves de condição para a Amazon DataZone

Ações definidas pela Amazon DataZone

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptPredictions	Concede permissão para aceitar previsões	Gravar			
AcceptSubscriptionRequest	Concede permissão para aprovar uma solicitação de assinatura de um ativo de dados	Gravar			
AddEntityOwner	Concede permissão para adicionar um proprietário a uma entidade como unidade de domínio	Gravar			
AddPolicyGrant	Concede permissão para adicionar uma concessão de política	Gerenciamento de permissões			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateEnvironmentRole	Concede permissão para associar uma função em um ambiente de esquema de serviço padrão	Gravar			
AssociateGovernedTerms	Concede permissão para associar termos governados a um ativo	Gravar			
BatchDeleteLinkedTypes [somente permissão]	Concede permissão para remover itens do tipo vinculado de um DataZone domínio da Amazon	Gravar	domain*		
BatchPutLinkedTypes [somente permissão]	Concede permissão para colocar itens do tipo vinculado em um DataZone domínio da Amazon	Gravar	domain*		
CancelMetadataGenerationRun	Concede permissão para cancelar a execução da geração de metadados	Gravar			
CancelSubscription	Concede permissão para revogar ou cancelar a assinatura aprovada do ativo de dados	Gravar			
CreateAccountPool	Concede permissão para criar um pool de contas	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAsset	Concede permissão para criar ativos	Gravar			
CreateAssetFilter	Concede permissão para criar um filtro de ativos	Gravar			
CreateAssetRevision	Concede permissão para criar uma nova revisão de um ativo	Gravar			
CreateAssetType	Concede permissão para criar um tipo de ativo	Gravar			
CreateConnection	Concede permissão para criar conexões	Gravar			
CreateDataProduct	Concede permissão para criar produtos de dados	Gravar			
CreateDataProductRevision	Concede permissão para criar revisão de produtos de dados	Gravar			
CreateDataSource	Concede permissão para criar um novo DataSource	Gravar			
CreateDomain	Concede permissão para provisionar um domínio que é uma entidade de nível superior que contém outros DataZone recursos da Amazon	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDomainUnit	Concede permissão para criar uma unidade de domínio	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateEnvironment	Concede permissão para criar uma coleção de recursos configurados, usados para publicar e assinar dados	Gravar			
CreateEnvironmentAction	Concede permissão para criar uma ação de ambiente em um ambiente de esquema de serviço padrão	Gravar			
CreateEnvironmentBlueprint [somente permissão]	Concede permissão para criar um esquema de ambiente personalizado que permite ao usuário adicionar ambientes ao seu projeto	Gravar			
CreateEnvironmentProfile	Concede permissão para criar um modelo a partir de um esquema que pode ser usado para criar um ambiente	Gravar			
CreateFormType	Concede permissão para criar um tipo de formulário ou uma nova revisão dele	Gravar			
CreateGlossary	Concede permissão para criar um glossário de negócios	Gravar			
CreateGlossaryTerm	Concede permissão para criar um termo de glossário	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateGroupProfile	Concede permissão para criar um perfil de DataZone grupo para um grupo do IAM Identity Center	Gravar			
CreateListingChangeSet	Concede permissão para criar um conjunto de alterações de listagem	Gravar			
CreateProject	Concede permissão para criar um projeto para possibilitar que sua equipe publique e assine dados	Gravar			
CreateProjectMembership	Concede permissão para adicionar um usuário a um projeto	Gravar			
CreateProjectProfile	Concede permissão para criar um perfil de projeto	Gravar			
CreateRule	Concede permissão para criar uma regra	Gravar			
CreateSubscriptionGrant	Concede permissão para criar uma concessão para uma assinatura aprovada em um destino de assinatura	Gravar			
CreateSubscriptionRequest	Concede permissão para criar uma solicitação de assinatura de um ativo de dados	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSubscriptionTarget	Concede permissão para criar um destino de assinatura para um ambiente no projeto	Gravar			
CreateUserProfile	Concede permissão para criar um perfil de usuário para um usuário existente no Centro de Identidade do IAM do cliente	Gravar			
DeleteAccountPool	Concede permissão para excluir um pool de contas	Gravar			
DeleteAsset	Concede permissão para excluir um ativo	Gravar			
DeleteAssetFilter	Concede permissão para excluir um filtro de ativos	Gravar			
DeleteAssetType	Concede permissão para excluir um tipo de ativo	Gravar			
DeleteConnection	Concede permissão para excluir conexões	Gravar			
DeleteDataProduct	Concede permissão para excluir produtos de dados	Gravar			
DeleteDataSource	Concede permissão para atualizar os existentes DataSource	Gravar			
DeleteDomain	Concede permissão para excluir um domínio provisionado	Gravar	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteDomainSharingPolicy [somente permissão]	Concede permissão para excluir uma política de recursos para um DataZone domínio	Gerenciamento de permissões			
DeleteDomainUnit	Concede permissão para excluir uma unidade de domínio existente	Gravar			
DeleteEnvironment	Concede permissão para excluir um ambiente	Gravar			
DeleteEnvironmentAction	Concede permissão para excluir uma ação de ambiente em um ambiente de esquema de serviço padrão	Gravar			
DeleteEnvironmentBlueprint [somente permissão]	Concede permissão para excluir um esquema de ambiente	Gravar			
DeleteEnvironmentBlueprintConfiguration	Concede permissão para excluir uma configuração de esquema de ambiente	Gravar			
DeleteEnvironmentProfile	Concede permissão para excluir um perfil ambiente	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteFormType	Concede permissão para excluir um tipo de formulário	Gravar			
DeleteGlossary	Concede permissão para excluir um glossário de negócios	Gravar			
DeleteGlossaryTerm	Concede permissão para excluir um termo de glossário	Gravar			
DeleteListing	Concede permissão para excluir uma listagem	Gravar			
DeleteProject	Concede permissão para excluir um projeto que possibilita que sua equipe publique e assine dados	Gravar			
DeleteProjectMembership	Concede permissão para remover um usuário de um projeto	Gravar			
DeleteProjectProfile	Concede permissão para excluir um perfil de projeto	Gravar			
DeleteRule	Concede permissão para excluir a regra	Gravar			
DeleteSubscriptionGrant	Concede permissão para excluir uma concessão de assinatura de um destino de assinatura	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteSubscriptionRequest	Concede permissão para excluir uma solicitação de assinatura pendente de um ativo de dados	Gravar			
DeleteSubscriptionTarget	Concede permissão para excluir um destino de assinatura de um ambiente no projeto	Gravar			
DeleteTimeSeriesDataPoints	Concede permissão para excluir os existentes TimeSeriesDataPoints	Gravar			
DisassociateEnvironmentRole	Concede permissão para desassociar uma função em um ambiente de esquema de serviço padrão	Gravar			
DisassociateGovernedTerms	Concede permissão para dissociar termos regulamentados de um ativo	Gravar			
GetAccountPool	Concede permissão para obter detalhes do pool de contas	Leitura			
GetAsset	Concede permissão para recuperar um ativo	Leitura			
GetAssetFilter	Concede permissão para obter um filtro de ativo	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAssetType	Concede permissão para obter um tipo de ativo	Leitura			
GetConnection	Concede permissão para obter conexões	Leitura			
GetDataProduct	Concede permissão para obter produtos de dados	Leitura			
GetDataSource	Concede permissão para obter um existente DataSource na Amazon DataZone usando seu identificador	Leitura			
GetDataSourceRun	Concede permissão para DataSource executar um trabalho na Amazon DataZone usando seu identificador	Leitura			
GetDomain	Concede permissão para recuperar informações sobre um domínio	Leitura	domain*		
GetDomainExecutionRoleCredentials [somente permissão]	Concede permissão para usar recursos que exigem acesso às credenciais da função de execução do domínio	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetDomainSharingPolicy [somente permissão]	Concede permissão para recuperar uma política de recursos para um DataZone domínio	Leitura			
GetDomainUnit	Concede permissão para obter uma unidade de domínio existente	Leitura			
GetEnvironment	Concede permissão para obter detalhes do ambiente	Leitura			
GetEnvironmentAction	Concede permissão para obter uma ação de ambiente em um ambiente de esquema de serviço padrão	Leitura			
GetEnvironmentActionLink [somente permissão]	Concede permissão para obter um link de ação de ambiente	Leitura			
GetEnvironmentBlueprint	Concede permissão para obter detalhes do esquema do ambiente	Leitura			
GetEnvironmentBlueprintConfiguration	Concede permissão para obter uma configuração de esquema de ambiente	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetEnvironmentCredentials	Concede permissão para obter credenciais de curto prazo que assumem o perfil de usuário do ambiente	Leitura			
GetEnvironmentProfile	Concede permissão para obter detalhes do perfil do ambiente	Leitura			
GetFormType	Concede permissão para obter um tipo de formulário	Leitura			
GetGlossary	Concede permissão para obter um glossário de negócios	Leitura			
GetGlossaryTerm	Concede permissão para obter um termo de glossário	Leitura			
GetGroupProfile	Concede permissão para recuperar um perfil de DataZone grupo existente	Leitura			
GetIamPortalLoginUrl	Concede permissão a um diretor do IAM para fazer login no DataZone Portal	Gerenciamento de permissões			
GetJobRun	Concede permissão para executar trabalhos	Leitura			
GetLineageEvent	Concede permissão para obter eventos de linhagem	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetLineageNode	Concede permissão para obter o nó de linhagem	Leitura			
GetListing	Concede permissão para obter uma listagem	Leitura			
GetMetadataGenerationRun	Concede permissão para obter a execução da geração de metadados	Leitura			
GetProject	Concede permissão para obter detalhes do projeto	Leitura			
GetProjectProfile	Concede permissão para obter detalhes do perfil do projeto	Leitura			
GetRule	Concede permissão para obter a regra	Leitura			
GetSubscription	Concede permissão para recuperar uma assinatura	Leitura			
GetSubscriptionEligibility [somente permissão]	Concede permissão para obter qualificação para a assinatura	Leitura			
GetSubscriptionGrant	Concede permissão para recuperar uma concessão de assinatura	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSubscriptionRequestDetails	Concede permissão para rejeitar uma solicitação de assinatura de um ativo de dados	Leitura			
GetSubscriptionTarget	Concede permissão para recuperar os detalhes de um destino de assinatura	Leitura			
GetTimeSeriesDataPoint	Concede permissão para obter um existente TimeSeriesDataPoints na Amazon DataZone usando seu identificador	Leitura			
GetUpdateEligibility	Concede permissão para obter o status de elegibilidade atualizado para construções de projetos	Leitura			
GetUserProfile	Concede permissão para recuperar um perfil de usuário para um usuário existente no Domínio DataZone	Leitura			
ListAccountEnvironments	Concede permissão para listar ambientes em todos os domínios em uma conta AWS	Lista			
ListAccountPools	Concede permissão para listar grupos de contas	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAccountsInAccountPool	Concede permissão para listar contas em um pool de contas	Lista			
ListAssetFilters	Concede permissão para listar filtros de ativos	Lista			
ListAssetRevisions	Concede permissão para listar revisões de um ativo	Lista			
ListConnections	Concede permissão para listar conexões	Lista			
ListDataProductRevisions	Concede permissão para listar revisões de produtos de dados	Lista			
ListDataSourceRunActivities	Concede permissão para listar as atividades do trabalho DataSource executado no Asset	Lista			
ListDataSourceRuns	Concede permissão para listar DataSource executa o trabalho	Lista			
ListDataSources	Concede permissão para listar os existentes DataSources	Lista			
ListDomainUnitsForParent	Concede permissão para listar unidades de domínio secundárias para uma determinada unidade de domínio principal	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDomains	Concede permissão para recuperar todos os domínios	Lista			
ListEntityOwners	Concede permissão para listar os proprietários de uma entidade como unidade de domínio	Lista			
ListEnvironmentActions	Concede permissão para listar ações de ambiente em um ambiente de esquema de serviço padrão	Lista			
ListEnvironmentBlueprintConfigurationSummaries [somente permissão]	Concede permissão para listar resumos de configuração de esquema do ambiente	Lista			
ListEnvironmentBlueprintConfigurations	Concede permissão para listar configurações de esquema de ambiente	Lista			
ListEnvironmentBlueprints	Concede permissão para listar o domínio para esquemas de ambiente	Lista			
ListEnvironmentProfiles	Concede permissão para listar o domínio para perfis de ambiente	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListEnvironments	Concede permissão para mostrar ambientes no domínio	Lista			
ListGroupsForUser	Concede permissão para listar todos os perfis de DataZone grupo dos DataZone quais o perfil do usuário é membro	Lista			
ListJobRuns	Concede permissão para listar execuções de trabalhos	Lista			
ListLineageEvents	Concede permissão para listar eventos de linhagem	Lista			
ListLineageNodeHistory	Concede permissão para listar versões históricas do nó de linhagem	Lista			
ListLinkedTypes [somente permissão]	Concede permissão para listar itens do tipo vinculado vinculados a um DataZone domínio da Amazon	Lista	domain*		
ListMetadataGenerationRuns	Concede permissão para listar execuções de gerações de metadados	Lista			
ListNotifications	Concede permissão para listar notificações e eventos para um usuário do DataZone	Lista			
ListPolicyGrants	Concede permissão para listar as concessões de políticas	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListProjectMemberships	Concede permissão para listar membros de projetos	Lista			
ListProjectProfiles	Concede permissão para listar perfis de projetos	Lista			
ListProjects	Concede permissão para listar projetos	Lista			
ListRules	Concede permissão para listar regras	Lista			
ListSubscriptionGrants	Concede permissão para listar concessões de assinatura para uma entidade principal inscrita	Lista			
ListSubscriptionRequests	Concede permissão para listar solicitações de assinatura	Lista			
ListSubscriptionTargets	Concede permissão para listar destinos de assinatura	Lista			
ListSubscriptions	Concede permissão para listar assinaturas	Lista			
ListTagsForResource	Concede permissão para recuperar todas as etiquetas associadas a um recurso	Leitura	domain		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTimeSeriesDataPoints	Concede permissão para listar os existentes TimeSeriesDataPoints	Lista			
ListWarehouseMetadata [somente permissão]	Concede permissão para listar segredos de gerenciador disponíveis	Lista			
PostLineageEvent	Concede permissão para publicar eventos de linhagem	Gravar			
PostTimeSeriesDataPoints	Concede permissão para publicar um novo TimeSeriesDataPoints	Gravar			
ProvisionDomain [somente permissão]	Concede permissão para provisionar o domínio com a configuração de projeto padrão	Gravar			
PutDomainSharingPolicy [somente permissão]	Concede permissão para adicionar uma política de recursos para um DataZone domínio	Gerenciamento de permissões			
PutEnvironmentBlueprintConfiguration	Concede permissão para colocar uma configuração de esquema de ambiente	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RefreshToken [somente permissão]	Concede permissão para atualizar um token	Gravar			
RejectPredictions	Concede permissão para rejeitar uma previsão	Gravar			
RejectSubscriptionRequest	Concede permissão para rejeitar uma solicitação de assinatura de um ativo de dados	Gravar			
RemoveEntityOwner	Concede permissão para remover um proprietário existente de uma entidade como unidade de domínio	Gravar			
RemovePolicyGrant	Concede permissão para remover uma concessão de política	Gerenciamento de permissões			
RevokeSubscription	Concede permissão para revogar uma assinatura	Gerenciamento de permissões			
Search	Concede permissão para pesquisar entidades do DataZone	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SearchGroupProfiles	Concede permissão para pesquisar perfis de DataZone grupos e grupos do IAM Identity Center	Lista			
SearchListings	Concede permissão para pesquisar listagens	Lista			
SearchRules [somente permissão]	Concede permissão para pesquisar regras	Lista			
SearchTypes	Concede permissão para pesquisar tipos como tipos de ativos e tipos de formulários em um domínio	Lista			
SearchUserProfiles	Concede permissão para pesquisar perfis de DataZone usuário, usuários do IAM Identity Center e perfis principais DataZone do IAM	Lista			
SsoLogin [somente permissão]	Concede permissão para fazer login usando o SSO	Gravar			
SsoLogout [somente permissão]	Concede permissão para fazer logout usando o SSO	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartAccountBootstrapAction [somente permissão]	Concede permissão para iniciar a ação de bootstrap da conta para um domínio	Gravar			
StartDataSourceRun	Concede permissão para iniciar um trabalho DataSource executado	Gravar			
StartMetadataGenerationRun	Concede permissão para iniciar a execução da geração de metadados	Gravar			
StopMetadataGenerationRun	Concede permissão para interromper a execução da geração de metadados	Gravar			
TagResource	Concede permissão para adicionar ou atualizar etiquetas em um recurso	Tags	domain*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover etiquetas associadas a um recurso	Tags	domain*		
				aws:TagKeys	
UpdateAccountPool	Concede permissão para atualizar um pool de contas	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateAssetFilter	Concede permissão para atualizar um filtro de ativos	Gravar			
UpdateConnection	Concede permissão para atualizar conexões	Gravar			
UpdateDataSource	Concede permissão para atualizar os existentes DataSource	Gravar			
UpdateDataSourceRunActivities [somente permissão]	Concede permissão para atualizar atividades de execução de fonte de dados	Gravar			
UpdateDomain	Concede permissão para atualizar informações de um domínio	Gravar	domain*		
UpdateDomainUnit	Concede permissão para atualizar uma unidade de domínio existente	Gravar			
UpdateEnvironment	Concede permissão para atualizar configurações do ambiente	Gravar			
UpdateEnvironmentAction	Concede permissão para atualizar uma ação de ambiente em um ambiente de esquema de serviço padrão	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateEnvironmentBlueprint [somente permissão]	Concede permissão para atualizar configurações de esquema do ambiente	Gravar			
UpdateEnvironmentConfiguration [somente permissão]	Concede permissão para atualizar uma configuração de ambiente	Gravar			
UpdateEnvironmentDeploymentStatus [somente permissão]	Concede permissão para atualizar o status da implantação do ambiente	Gravar			
UpdateEnvironmentProfile	Concede permissão para atualizar a EnvironmentProfile configuração	Gravar			
UpdateGlossary	Concede permissão para atualizar um glossário de negócios	Gravar			
UpdateGlossaryTerm	Concede permissão para atualizar um termo de glossário	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateGroupProfile	Concede permissão para atualizar um perfil de DataZone grupo	Gravar			
UpdateProject	Concede permissão para atualizar um projeto que possibilita que sua equipe publique e assine dados	Gravar			
UpdateProjectProfile	Concede permissão para atualizar um perfil de projeto	Gravar			
UpdateRule	Concede permissão para atualizar a regra	Gravar			
UpdateSubscriptionGrantStatus	Concede permissão para atualizar o status de uma concessão de assinatura para concessões personalizadas	Gravar			
UpdateSubscriptionRequest	Concede permissão para atualizar o motivo de negócios da solicitação de assinatura para um ativo de dados	Gravar			
UpdateSubscriptionTarget	Concede permissão para atualizar o destino de uma assinatura	Gravar			
UpdateUserProfile	Concede permissão para atualizar um perfil de DataZone usuário	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ValidatePassRole [somente permissão]	Concede permissão para validar um perfil de aprovação	Gravar			

Tipos de recursos definidos pela Amazon DataZone

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
domain	`arn:${Partition}:datazone:${Region}:${Account}:domain/${DomainId}`	aws:ResourceTag/${TagKey}

Chaves de condição para a Amazon DataZone

A Amazon DataZone define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString
datazone:domainId	Filtra o acesso pelo ID de domínio passado na solicitação	String
datazone:projectId	Filtra o acesso pelo ID do projeto passado na solicitação	String
datazone:userId	Filtra o acesso pelo ID de usuário passado na solicitação	String

Ações, recursos e chaves de condição do AWS Deadline Cloud

AWS O Deadline Cloud (prefixo do serviço:`deadline`) fornece os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Deadline Cloud
- Tipos de recursos definidos pelo AWS Deadline Cloud
- Chaves de condição do AWS Deadline Cloud

Ações definidas pelo AWS Deadline Cloud

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateMemberToFarm	Concede permissão para associar um membro a um farm	Gerenciamento de permissões	farm*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel deadline:MembershipLevel	
AssociateMemberToFleet	Concede permissão para associar um membro a uma frota	Gerenciamento de permissões	fleet*		identitystore:DescribeGroup identitystore:DescribeUser

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel deadline:MembershipLevel	
AssociateMemberToJob	Concede permissão para associar um membro a um trabalho	Gerenciamento de permissões	job*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				deadline:AssociatedMembershipLevel deadline:MembershipLevel	
AssociateMemberToQueue	Concede permissão para associar um membro a uma fila	Gerenciamento de permissões	queue*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel deadline:MembershipLevel	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssumeFleetRoleForRead	Concede permissão para assumir uma função de frota para acesso somente leitura	Gravar	fleet*		identitystore:ListGroupMembershipsForMember
AssumeFleetRoleForWorker	Concede permissão para assumir uma função de frota para um trabalhador	Gravar	worker*		
AssumeQueueRoleForRead	Concede permissão para assumir uma função de fila para acesso somente leitura	Gravar	queue*		identitystore:ListGroupMembershipsForMember
AssumeQueueRoleForUser	Concede permissão para assumir uma função de fila para um usuário	Gravar	queue*		identitystore:ListGroupMembershipsForMember
AssumeQueueRoleForWorker	Concede permissão para assumir uma função de fila para um trabalhador	Gravar	queue* worker*		
BatchGetJobEntity	Concede permissão para obter uma entidade de trabalho para um trabalhador	Leitura	worker*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CopyJobTemplate	Concede permissão para copiar um modelo de trabalho para um bucket do Amazon S3	Gravar	job*		identitystore:ListGroupMembershipsForMember s3:PutObject
CreateBudget	Concede permissão para criar um orçamento	Gravar	budget*		identitystore:ListGroupMembershipsForMember
CreateFarm	Concede permissão para criar uma farm	Gravar	farm*		deadline:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateFleet	Concede permissão para criar uma frota	Gravar	fleet*		deadline:TagResource ec2:CreateVpcEndpoint iam:PassRole identitystore:ListGroupMembershipsForMember logs:CreateLogGroup vpc-lattice:GetResourceConfiguration vpc-lattice:GetResourceGateway

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateJob	Concede permissão para criar um trabalho	Gravar	job*		deadline:GetJobTemplate identitystore:ListGroupMembershipsForMember
CreateLicenseEndpoint	Concede permissão para criar um endpoint de licença para software ou produtos licenciados	Gravar	license-endpoint*		deadline:TagResource ec2:CreateTags ec2:CreateVpcEndpoint ec2:DescribeVpcEndpoints

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLimit	Concede permissão para criar um limite para uma fazenda	Gravar	farm*		identitystore:ListGroupMembershipsForMember

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateMonitor	Concede permissão para criar um monitor	Gravar	monitor*		deadline:TagResource iam:PassRole sso:CreateApplication sso:DeleteApplication sso:PutApplicationAssignmentConfiguration sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateQueue	Concede permissão para criar uma fila	Gravar	queue*		deadline:TagResource iam:PassRole identitystore:ListGroupMembershipsForMember logs:CreateLogGroup s3:ListBucket
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateQueueEnvironment	Concede permissão para criar um ambiente de fila	Gravar	queue*		identitystore:ListGroupMembershipsForMember
CreateQueueFleetAssociation	Concede permissão para criar uma associação de frota e filas	Gravar	fleet*		identitystore:ListGroupMembershipsForMember
			queue*		
CreateQueueLimitAssociation	Concede permissão para criar uma associação de limite de fila	Gravar	farm*		identitystore:ListGroupMembershipsForMember
			queue*		
CreateStorageProfile	Concede permissão para criar um perfil de armazenamento para um farm	Gravar	farm*		identitystore:ListGroupMembershipsForMember

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateWorker	Concede permissão para criar um operador	Gravar	worker*		deadline:ListTagsForResource deadline:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBudget	Concede permissão para excluir um orçamento	Gravar	budget*		identitystore:ListGroupMembershipsForMember
DeleteFarm	Concede permissão para excluir uma farm	Gravar	farm*		identitystore:ListGroupMembershipsForMember
DeleteFleet	Concede permissão para excluir uma frota	Gravar	fleet*		identitystore:ListGroupMembershipsForMember

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteLicenseEndpoint	Concede permissão para excluir um endpoint de licença	Gravar	license-endpoint*		ec2:DeleteVpcEndpoints ec2:DescribeVpcEndpoints
DeleteLimit	Concede permissão para excluir um limite	Gravar	farm*		identitystore:ListGroupMembershipsForMember
DeleteMeteredProduct	Concede permissão para excluir um produto mensurado	Gravar	metered-product*		
DeleteMonitor	Concede permissão para excluir um monitor	Gravar	monitor*		sso:DeleteApplication
DeleteQueue	Concede permissão para excluir uma fila	Gravar	queue*		identitystore:ListGroupMembershipsForMember
DeleteQueueEnvironment	Concede permissão para excluir um ambiente de fila	Gravar	queue*		identitystore:ListGroupMembershipsForMember

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteQueueFleetAssociation	Concede permissão para excluir uma associação de frota e filas	Gravar	fleet*		identitystore:ListGroupMembershipsForMember
			queue*		
DeleteQueueLimitAssociation	Concede permissão para excluir uma associação de limite de fila	Gravar	farm*		identitystore:ListGroupMembershipsForMember
			queue*		
DeleteStorageProfile	Concede permissão para excluir um perfil de armazenamento	Gravar	farm*		identitystore:ListGroupMembershipsForMember
DeleteWorker	Concede permissão para excluir um operador	Gravar	worker*		
DisassociateMemberFromFarm	Concede permissão para desassociar um membro de uma farm	Gerenciamento de permissões	farm*		identitystore:ListGroupMembershipsForMember

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				deadline:AssociatedMembershipLevel	
DisassociateMemberFromFleet	Concede permissão para desassociar um membro de uma frota	Gerenciamento de permissões	fleet*		identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel	
DisassociateMemberFromJob	Concede permissão para desassociar um membro de um trabalho	Gerenciamento de permissões	job*		identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel	
DisassociateMemberFromQueue	Concede permissão para desassociar um membro de uma fila	Gerenciamento de permissões	queue*		identitystore:ListGroupMembershipsForMember

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				deadline:AssociatedMembershipLevel	
GetApplicationVersion	Concede permissão para obter a versão mais recente de uma aplicação	Leitura	monitor*		
GetBudget	Concede permissão para obter um orçamento	Leitura	budget*		identitystore:ListGroupMembershipsForMember
GetFarm	Concede permissão para obter uma farm	Leitura	farm*		identitystore:ListGroupMembershipsForMember
GetFleet	Concede permissão para obter uma frota	Leitura	fleet*		identitystore:ListGroupMembershipsForMember
GetJob	Concede permissão para obter um trabalho	Leitura	job*		identitystore:ListGroupMembershipsForMember

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetJobTemplate [somente permissão]	Concede permissão para ler um modelo de trabalho	Leitura	job*		
GetLicenseEndpoint	Concede permissão para obter um endpoint de licença	Leitura	license-endpoint*		
GetLimit	Concede permissão para obter um limite	Leitura	farm*		identitystore:ListGroupMembershipsForMember
GetMonitor	Concede permissão para obter um monitor	Leitura	monitor*		
GetQueue	Concede permissão para obter uma fila	Leitura	queue*		identitystore:ListGroupMembershipsForMember
GetQueueEnvironment	Concede permissão para obter um ambiente de fila	Leitura	queue*		identitystore:ListGroupMembershipsForMember

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetQueueFleetAssociation	Concede permissão para obter uma associação de frota e filas	Leitura	fleet*		identitystore:ListGroupMembershipsForMember
			queue*		
GetQueueLimitAssociation	Concede permissão para obter uma associação de limite de fila	Leitura	farm*		identitystore:ListGroupMembershipsForMember
			queue*		
GetSession	Concede permissão para obter uma sessão de um trabalho	Leitura	job*		identitystore:ListGroupMembershipsForMember
GetSessionAction	Concede permissão para obter uma ação de sessão para um trabalho	Leitura	job*		identitystore:ListGroupMembershipsForMember
GetSessionsStatisticsAggregation	Concede permissão para obter todas as estatísticas coletadas para sessões	Leitura	farm		identitystore:ListGroupMembershipsForMember

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			fleet		
			queue		
GetStep	Concede permissão para obter uma etapa em um trabalho	Leitura	job*		identitystore:ListGroupMembershipsForMember
GetStorageProfile	Concede permissão para obter um perfil de armazenamento	Leitura	farm*		identitystore:ListGroupMembershipsForMember
GetStorageProfileForQueue	Concede permissão para obter um perfil de armazenamento para uma fila	Leitura	queue*		identitystore:ListGroupMembershipsForMember
GetTask	Concede permissão para obter uma tarefa de trabalho	Leitura	job*		identitystore:ListGroupMembershipsForMember
GetWorker	Concede permissão para obter um operador	Leitura	worker*		identitystore:ListGroupMembershipsForMember

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAvailableMeteredProducts	Concede permissão para listar todos os produtos mensurados disponíveis em um endpoint de licença	Lista			
ListBudgets	Concede permissão para listar todos os orçamentos de farms	Lista	budget*		identitystore:ListGroupMembershipsForMember
ListFarmMembers	Concede permissão para listar todos os membros de uma farm	Lista	farm*		identitystore:ListGroupMembershipsForMember
ListFarms	Concede permissão para listar todas as farms	Lista	farm*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				deadline:PrincipalId deadline:RequesterPrincipalId	
ListFleetMembers	Concede permissão para listar todos os membros de uma frota	Lista	fleet*		identitystore:ListGroupMembershipsForMember
ListFleets	Concede permissão para listar todas as frotas	Lista	fleet*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				deadline:PrincipalId deadline:RequesterPrincipalId	
ListJobMembers	Concede permissão para listar todos os membros de um trabalho	Lista	job*		identitystore:ListGroupMembershipsForMember
ListJobParameterDefinitions	Concede permissão para obter as definições de parâmetros de um trabalho no modelo de trabalho	Lista	job*		identitystore:ListGroupMembershipsForMember

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListJobs	Concede permissão para listar todos os trabalhos em uma fila	Lista	job*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:PrincipalId deadline:RequesterPrincipalId	
ListLicenseEndpoints	Concede permissão para listar todos os endpoints de licença	Lista	license-endpoint*		
ListLimits	Concede permissão para listar todos os limites em uma fazenda	Lista	farm*		identitystore:ListGroupMembershipsForMember

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListMeteredProducts	Concede permissão para listar todos os produtos mensurados em um endpoint de licença	Lista	metered-product*		
ListMonitors	Concede permissão para listar todos os monitores	Lista	monitor*		
ListQueueEnvironments	Concede permissão para listar todos os ambientes de fila aos quais uma fila está associada	Lista	queue*		identitystore:ListGroupMembershipsForMember
ListQueueFleetAssociations	Concede permissão para listar todas as associações de frota e filas	Lista	farm*		identitystore:ListGroupMembershipsForMember
			fleet*		
			queue*		
ListQueueLimitAssociations	Concede permissão para listar todas as associações de limite de fila	Lista	farm*		identitystore:ListGroupMembershipsForMember
			queue*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListQueueMembers	Concede permissão para listar todos os membros em uma fila	Lista	queue*		identitystore:ListGroupMembershipsForMember
ListQueues	Concede permissão para listar todas as filas em farms	Lista	queue*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:PrincipalId deadline:RequesterPrincipalId	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListSessionActions	Concede permissão para listar todas as ações da sessão de um trabalho	Lista	job*		identitystore:ListGroupMembershipsForMember
ListSessions	Concede permissão para listar todas as sessões de um trabalho	Lista	job*		identitystore:ListGroupMembershipsForMember
ListSessionsForWorker	Concede permissão para listar todas as sessões de um trabalhador	Lista	worker*		identitystore:ListGroupMembershipsForMember
ListStepConsumers	Concede permissão para listar os consumidores de uma etapa de trabalho	Lista	job*		identitystore:ListGroupMembershipsForMember
ListStepDependencies	Concede permissão para listar dependências de uma etapa de trabalho	Lista	job*		identitystore:ListGroupMembershipsForMember

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListSteps	Concede permissão para listar todas as etapas de um trabalho	Lista	job*		identitystore:ListGroupMembershipsForMember
ListStorageProfiles	Concede permissão para listar todos os perfis de armazenamento em farms	Lista	farm*		identitystore:ListGroupMembershipsForMember
ListStorageProfilesForQueue	Concede permissão para listar todos os perfis de armazenamento em uma fila	Lista	queue*		identitystore:ListGroupMembershipsForMember
ListTagsForResource	Concede permissão para listar todas as tags em recursos especificados do Deadline Cloud	Lista	farm		
			fleet		
			license-endpoint		
			monitor		
			queue		
			worker		
				deadline:CalledAction	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTasks	Concede permissão para listar todas as tarefas de um trabalho	Lista	job*		identitystore:ListGroupMembershipsForMember
ListWorkers	Concede permissão para listar todos os trabalhadores em uma frota	Lista	worker*		identitystore:ListGroupMembershipsForMember
PutMeteredProduct	Concede permissão para adicionar um produto mensurado a um endpoint de licença	Gravar	metered-product*		
SearchJobs	Concede permissão para pesquisar trabalhos em várias filas	Lista	queue*		identitystore:ListGroupMembershipsForMember
SearchSteps	Concede permissão para pesquisar as etapas em um único trabalho ou em várias filas	Lista	job		identitystore:ListGroupMembershipsForMember
			queue		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SearchTasks	Concede permissão para pesquisar as tarefas em um único trabalho ou em várias filas	Lista	job		identitystore:ListGroupMembershipsForMember
			queue		
SearchWorkers	Concede permissão para pesquisar trabalhadores em várias frotas	Lista	fleet*		identitystore:ListGroupMembershipsForMember
StartSessionsStatisticsAggregation	Concede permissão para obter todas as estatísticas coletadas para sessões	Leitura	fleet		identitystore:ListGroupMembershipsForMember
			queue		
TagResource	Concede permissão para adicionar ou substituir uma ou mais tags do recurso especificado do Deadline Cloud	Tags	farm		
			fleet		
			license-endpoint		
			monitor		
			queue		
			worker		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys deadline:CalledAction	
UntagResource	Concede permissão para desassociar uma ou mais tags do recurso especificado do Deadline Cloud	Tags	farm		
			fleet		
			license-endpoint		
			monitor		
			queue		
			worker		
				aws:TagKeys	
UpdateBudget	Concede permissão para atualizar um orçamento	Gravar	budget*		identitystore:ListGroupMembershipsForMember

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateFarm	Concede permissão para atualizar uma farm	Gravar	farm*		identitystore:ListGroupMembershipsForMember
UpdateFleet	Concede permissão para atualizar uma frota	Gravar	fleet*		ec2:CreateVpcEndpoint iam:PassRole identitystore:ListGroupMembershipsForMember vpc-lattice:GetResourceConfiguration vpc-lattice:GetResourceGateway

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateJob	Concede permissão para atualizar um trabalho	Gravar	job*		identitystore:ListGroupMembershipsForMember
UpdateLimit	Concede permissão para atualizar um limite para uma fazenda	Gravar	farm*		identitystore:ListGroupMembershipsForMember
UpdateMonitor	Concede permissão para atualizar um monitor	Gravar	monitor*		iam:PassRole sso:PutApplicationGrant sso:UpdateApplication
UpdateQueue	Concede permissão para atualizar uma fila	Gravar	queue*		iam:PassRole identitystore:ListGroupMembershipsForMember

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateQueueEnvironment	Concede permissão para atualizar um ambiente de fila	Gravar	queue*		identitystore:ListGroupMembershipsForMember
UpdateQueueFleetAssociation	Concede permissão para atualizar uma associação de frota e filas	Gravar	fleet*		identitystore:ListGroupMembershipsForMember
			queue*		
UpdateQueueLimitAssociation	Concede permissão para atualizar uma associação de limite de fila	Gravar	farm*		identitystore:ListGroupMembershipsForMember
			queue*		
UpdateSession	Concede permissão para atualizar uma sessão de um trabalho	Gravar	job*		identitystore:ListGroupMembershipsForMember
UpdateStep	Concede permissão para atualizar uma etapa de um trabalho	Gravar	job*		identitystore:ListGroupMembershipsForMember

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateStorageProfile	Concede permissão para atualizar um perfil de armazenamento para farms	Gravar	farm*		identitystore:ListGroupMembershipsForMember
UpdateTask	Concede permissão para atualizar uma tarefa	Gravar	job*		identitystore:ListGroupMembershipsForMember
UpdateWorker	Concede permissões para atualizar um operador	Gravar	worker*		logs:CreateLogStream
UpdateWorkerSchedule	Concede permissão para atualizar a programação de um trabalhador	Gravar	worker*		logs:CreateLogStream

Tipos de recursos definidos pelo AWS Deadline Cloud

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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
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}	

Tipos de recursos	ARN	Chaves de condição
monitor	`arn:${Partition}:deadline:${Region}:${Account}:monitor/${MonitorId}`	aws:ResourceTag/${TagKey}
queue	`arn:${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

Chaves de condição do AWS Deadline Cloud

AWS O Deadline Cloud define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString
deadline:AssociatedMembershipLevel	Filtra o acesso pelo nível de associação relacionado à entidade principal fornecida na solicitação	String
deadline:CalledAction	Filtra o acesso pela ação permitida na solicitação	String
deadline:FarmMembershipLevels	Filtra o acesso por níveis de associação em farms	ArrayOfString
deadline:FleetMembershipLevels	Filtra o acesso por níveis de associação na frota	ArrayOfString
deadline:JobMembershipLevels	Filtra o acesso por níveis de associação no trabalho	ArrayOfString
deadline:MembershipLevel	Filtra o acesso pelo nível de associação transmitido na solicitação	String
deadline:PrincipalId	Filtra o acesso pelo ID principal fornecido na solicitação	String

Chaves de condição	Descrição	Tipo
deadline:QueueMembershipLevels	Filtra o acesso por níveis de associação na fila	ArrayOfString
deadline:RequesterPrincipalId	Filtra o acesso do usuário que chama a API do Deadline Cloud	String

Ações, recursos e chaves de condição para o AWS DeepComposer

AWS DeepComposer (prefixo do serviço:`deepcomposer`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS DeepComposer
- Tipos de recursos definidos pelo AWS DeepComposer
- Chaves de condição do AWS DeepComposer

Ações definidas pelo AWS DeepComposer

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateCoupon [somente permissão]	Concede permissão para associar um DeepComposer cupom (ou DSN) à conta associada ao remetente da solicitação	Gravar			
CreateAudio [somente permissão]	Concede permissão para criar um arquivo de áudio convertendo a composição midi em um arquivo wav ou mp3.	Write	audio*		
CreateComposition [somente permissão]	Concede permissão para criar uma composição midi de várias faixas.	Write	composition*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModel [somente permissão]	Concede permissão para iniciar creating/training um modelo generativo capaz de realizar inferências com a melodia de piano fornecida pelo usuário para criar uma composição midi de várias faixas	Gravar	model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteComposition	Concede permissão para excluir a composição.	Write	composition*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
[somente permissão]					
DeleteModel	Concede permissão para excluir o modelo.	Write	model*		
GetComposition [somente permissão]	Concede permissão para obter informações sobre a composição.	Read	composition*		
				aws:ResourceTag/${TagKey}	
GetModel [somente permissão]	Concede permissão para obter informações sobre o modelo.	Read	model*		
				aws:ResourceTag/${TagKey}	
GetSampleModel [somente permissão]	Concede permissão para obter informações sobre a DeepComposer amostra/modelo pré-treinado	Leitura	model*		
ListCompositions [somente permissão]	Concede permissão para listar todas as composições de propriedade do remetente da solicitação.	List	composition*		
ListModels [somente permissão]	Concede permissão para listar todos os modelos de propriedade do remetente da solicitação.	List	model*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListSampleModels [somente permissão]	Concede permissão para listar todas as amostras/modelos pré-treinados fornecidos pelo serviço DeepComposer	Lista	model*		
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	List	composition		
			model		
				aws:ResourceTag/${TagKey}	
ListTrainingTopics [somente permissão]	Concede permissão para listar todas as opções de treinamento ou tópico de creating/training um modelo	Lista	model*		
TagResource	Concede permissão para marcar um recurso	Marcação	composition		
			model		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para desmarcar um recurso	Marcação	composition		
			model		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateComposition [somente permissão]	Concede permissão para modificar as propriedades mutáveis associadas a uma composição.	Write	composition*		
UpdateModel [somente permissão]	Concede permissão para modificar as propriedades mutáveis associadas a um modelo.	Gravar	model*		

Tipos de recursos definidos pelo AWS DeepComposer

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}`	

Chaves de condição do AWS DeepComposer

AWS DeepComposer define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por ações com base na presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por ações com base nos pares de chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso por ações com base na presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS DeepRacer

AWS DeepRacer (prefixo do serviço:`deepracer`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS DeepRacer
- Tipos de recursos definidos pelo AWS DeepRacer
- Chaves de condição do AWS DeepRacer

Ações definidas pelo AWS DeepRacer

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddLeaderboardAccessPermission [somente permissão]	Concede permissão para adicionar acesso a um placar de classificação privado	Write	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
AdminDescribeAccountKey	Concede permissão para recuperar informações da chave KMS que o usuário	Leitura		deepracer:UserToken	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
[somente permissão]	atualmente atribuiu à sua conta			deepracer:MultiUser	
AdminGetAccountConfig [somente permissão]	Concede permissão para obter a configuração atual de multiusuário administrador para esta conta	Leitura			
AdminListAssociatedResources [somente permissão]	Concede permissão para listar todos os usuários deepracer com seus recursos associados criados dentro desta conta	Leitura			
AdminListAssociatedUsers [somente permissão]	Concede permissão para listar dados de usuário para todos os usuários associados a esta conta	Leitura			
AdminManageUser [somente permissão]	Concede permissão para gerenciar um usuário associado a essa conta	Gravar			
AdminSetAccountConfig [somente permissão]	Concede permissão para definir opções de configuração para esta conta	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AdminUpdateAccountKey [somente permissão]	Concede permissão para atualizar a chave KMS atribuída à conta do usuário	Gravar		deepracer:UserToken deepracer:MultiUser	
CloneReinforcementLearningModel [somente permissão]	Concede permissão para clonar um modelo existente DeepRacer	Gravar	reinforcement_learning_model*		
			track*		
				aws:RequestTag/${TagKey} aws:TagKeys deepracer:UserToken deepracer:MultiUser	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateCar [somente permissão]	Concede permissão para criar um DeepRacer carro em sua garagem	Gravar		aws:RequestTag/${TagKey} aws:TagKeys deepracer:UserToken deepracer:MultiUser	
CreateLeaderboard [somente permissão]	Concede permissão para criar um placar	Write		aws:RequestTag/${TagKey} aws:TagKeys deepracer:UserToken deepracer:MultiUser	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateLeaderboardAccessToken [somente permissão]	Concede permissão para criar um token de acesso para um placar privado	Write	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
CreateLeaderboardSubmission [somente permissão]	Concede permissão para enviar um DeepRacer modelo para ser avaliado nas tabelas de classificação	Gravar	leaderboard*		
			reinforcement_learning_model*		
				aws:RequestTag/${TagKey} aws:TagKeys deepracer:UserToken deepracer:MultiUser	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateReinforcementLearningModel [somente permissão]	Concede permissão para criar um modelo de aprendizado por reforço bruto para DeepRacer	Gravar	track*		
				aws:RequestTag/${TagKey} aws:TagKeys deepracer:UserToken deepracer:MultiUser	
DeleteLeaderboard [somente permissão]	Concede permissão para excluir um placar	Write	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
DeleteModel [somente permissão]	Concede permissão para excluir um DeepRacer modelo	Gravar	reinforcement_learning_model*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				deepracer:UserToken deepracer:MultiUser	
EditLeaderboard [somente permissão]	Concede permissão para editar um placar	Write	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
GetAccountConfig [somente permissão]	Concede permissão para obter a atual configuração multiusuário para esta conta	Leitura		deepracer:UserToken deepracer:MultiUser	
GetAlias [somente permissão]	Concede permissão para recuperar o alias do usuário para enviar um DeepRacer modelo às tabelas de classificação	Leitura		deepracer:UserToken deepracer:MultiUser	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAssetUrl [somente permissão]	Concede permissão para baixar artefatos para um modelo existente DeepRacer	Leitura	reinforcement_learning_model*		
				deepracer:UserToken deepracer:MultiUser	
GetCar [somente permissão]	Concede permissão para recuperar um DeepRacer carro específico da sua garagem	Leitura	car*		
				deepracer:UserToken deepracer:MultiUser	
GetCars [somente permissão]	Concede permissão para ver todos os DeepRacer carros em sua garagem	Leitura		deepracer:UserToken deepracer:MultiUser	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetEvaluation [somente permissão]	Concede permissão para recuperar informações sobre os trabalhos de avaliação de um DeepRacer modelo existente	Leitura	evaluation_job*		
				deepracer:UserToken deepracer:MultiUser	
GetLatestUserSubmission [somente permissão]	Concede permissão para recuperar informações sobre o desempenho do último DeepRacer modelo enviado por um usuário em uma tabela de classificação	Leitura	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
GetLeaderboard [somente permissão]	Concede permissão para recuperar informações sobre placares	Read	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetModel [somente permissão]	Concede permissão para recuperar informações sobre um modelo existente DeepRacer	Leitura	reinforcement_learning_model*		
				deepracer:UserToken deepracer:MultiUser	
GetPrivateLeaderboard [somente permissão]	Concede permissão para recuperar informações sobre placares privados	Read	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
GetRankedUserSubmission [somente permissão]	Concede permissão para recuperar informações sobre o desempenho do DeepRacer modelo de um usuário que foi colocado em uma tabela de classificação	Leitura	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetTrack [somente permissão]	Concede permissão para recuperar informações sobre faixas DeepRacer	Leitura	track*		
GetTrainingJob [somente permissão]	Concede permissão para recuperar informações sobre o trabalho de treinamento de um DeepRacer modelo existente	Leitura	training_job*		
				deepracer:UserToken deepracer:MultiUser	
ImportModel [somente permissão]	Concede permissão para importar um modelo de aprendizado por reforço para DeepRacer	Gravar		deepracer:UserToken deepracer:MultiUser	
ListEvaluations [somente permissão]	Concede permissão para listar os trabalhos de avaliação de um DeepRacer modelo	Leitura	reinforcement_learning_model*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				deepracer:UserToken deepracer:MultiUser	
ListLeaderboardEvaluations [somente permissão]	Concede permissão para listar todos os trabalhos de avaliação de placar do usuário para um placar	Leitura	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
ListLeaderboardSubmissions [somente permissão]	Concede permissão para listar todas as submissões de DeepRacer modelos de um usuário em uma tabela de classificação	Leitura	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListLeaderboards [somente permissão]	Concede permissão para listar todos os placares disponíveis	Read		deepracer:UserToken deepracer:MultiUser	
ListModels [somente permissão]	Concede permissão para listar todos os DeepRacer modelos existentes	Leitura		deepracer:UserToken deepracer:MultiUser	
ListPrivateLeaderboardParticipants [somente permissão]	Concede permissão para recuperar informações do participante sobre placares privados	Read	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
ListPrivateLeaderboards [somente permissão]	Concede permissão para listar todos os placares privados disponíveis	Read		deepracer:UserToken deepracer:MultiUser	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListSubscribedPrivateLeaderboards [somente permissão]	Concede permissão para listar todos os placares privados assinados	Leitura		deepracer:UserToken deepracer:MultiUser	
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	car		
			evaluation_job		
			leaderboard		
			leaderboard_evaluation_job		
			reinforcement_learning_model		
			training_job		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} deepracer:UserToken deepracer:MultiUser	
ListTracks [somente permissão]	Concede permissão para listar todas as DeepRacer faixas	Leitura			
ListTrainingJobs [somente permissão]	Concede permissão para listar os trabalhos de treinamento de um DeepRacer modelo	Leitura	reinforcement_learning_model*		
				deepracer:UserToken deepracer:MultiUser	
MigrateModels [somente permissão]	Concede permissão para migrar modelos anteriores de aprendizado por reforço para DeepRacer	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PerformLeaderboardOperation [somente permissão]	Concede permissão para executar a operação de placar mencionada no atributo de operação	Gravar	leaderboard		
				deepracer:UserToken deepracer:MultiUser	
RemoveLeaderboardAccessPermission [somente permissão]	Concede permissão para remover o acesso de um placar privado	Write	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
SetAlias [somente permissão]	Concede permissão para definir o alias do usuário para enviar um DeepRacer modelo às tabelas de classificação	Gravar		deepracer:UserToken deepracer:MultiUser	
StartEvaluation [somente permissão]	Concede permissão para avaliar um DeepRacer modelo em um ambiente simulado	Gravar	reinforcement_learning_model*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			track*		
				aws:RequestTag/${TagKey} aws:TagKeys deepracer:UserToken deepracer:MultiUser	
StopEvaluation [somente permissão]	Concede permissão para interromper as avaliações DeepRacer do modelo	Gravar	evaluation_job*		
				deepracer:UserToken deepracer:MultiUser	
StopTrainingReinforcementLearningModel [somente permissão]	Concede permissão para parar de treinar um DeepRacer modelo	Gravar	reinforcement_learning_model*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				deepracer:UserToken deepracer:MultiUser	
TagResource	Concede permissão para marcar um recurso	Marcação	car		
			evaluation_job		
			leaderboard		
			leaderboard_evaluation_job		
			reinforcement_learning_model		
			training_job		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} deepracer:UserToken deepracer:MultiUser	
TestRewardFunction [somente permissão]	Concede permissão para testar as funções de recompensa para correção	Gravar			
UntagResource	Concede permissão para desmarcar um recurso	Marcação	car		
			evaluation_job		
			leaderboard		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			leaderboard_evaluation_job		
			reinforcement_learning_model		
			training_job		
				aws:TagKeys deepracer:UserToken deepracer:MultiUser	
UpdateCar [somente permissão]	Concede permissão para atualizar um DeepRacer carro em sua garagem	Gravar	car*		
				deepracer:UserToken deepracer:MultiUser	

Tipos de recursos definidos pelo AWS DeepRacer

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}
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}

Chaves de condição do AWS DeepRacer

AWS DeepRacer define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta na solicitação	ArrayOfString
deepracer:MultiUser	Filtra o acesso por sinalizador multiusuário	Bool
deepracer:UserToken	Filtra o acesso por token de usuário na solicitação	String

Ações, recursos e chaves de condição do Amazon Detective

O Amazon Detective (prefixo do serviço: `detective`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Detective
- Tipos de recursos definidos pelo Amazon Detective
- Chaves de condição do Amazon Detective

Ações definidas pelo Amazon Detective

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptInvitation	Concede permissão para aceitar um convite para se tornar membro de um gráfico de comportamento	Gravar	Graph*		
BatchGetGraphMemberDatasources	Concede permissão para recuperar o histórico do pacote de fonte de dados especificado das contas de membro especificadas em um grafo de comportamento gerenciado por essa conta	Leitura	Graph*		
BatchGetMembershipDatasources	Concede permissão para recuperar o histórico do pacote de fonte de dados do autor da chamada da conta para os grafos especificados	Leitura			
CreateGraph	Concede permissão para criar um gráfico de comportam	Write		aws:TagKeys	detective:TagResource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	ento e começar a agregar informações de segurança			aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
CreateMembers	Concede permissão para solicitar a associação de uma ou mais contas em um gráfico de comportamento gerenciado por essa conta	Write	Graph*		
DeleteGraph	Concede permissão para excluir um gráfico de comportamento e interromper a agregação de informações de segurança	Write	Graph*		
DeleteMembers	Concede permissão para remover contas-membro de um gráfico de comportamento gerenciado por essa conta	Gravar	Graph*		
DescribeOrganizationConfiguration	Concede permissão para visualizar a configuração atual relacionada à integração do Amazon Detective com Organizations AWS	Leitura	Graph*		organizations:DescribeOrganization

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisableOrganizationAdminAccount	Concede permissão para remover a conta de administrador delegado do Amazon Detective de uma organização	Gravar			organizations:DescribeOrganization
DisassociateMembership	Concede permissão para remover a associação dessa conta a um gráfico de comportamento	Gravar	Graph*		
EnableOrganizationAdminAccount	Concede permissão para designar a conta de administrador delegado do Amazon Detective para uma organização	Gravar			iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:EnableAWSServiceAccess organizations:RegisterDelegatedAdministrator

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetFreeTrialEligibility [somente permissão]	Concede permissão para recuperar a elegibilidade de um gráfico de comportamento para um período de avaliação gratuita	Read	Graph*		
GetGraphIngestState [somente permissão]	Concede permissão para recuperar o estado de ingestão de dados de um gráfico de comportamento	Leitura	Graph*		
GetInvestigation	Concede permissão para obter o status e os metadados de uma investigação	Leitura	Graph*		
GetMembers	Concede permissão para recuperar detalhes sobre membros especificados de um gráfico de comportamento	Read	Graph*		
GetPricingInformation [somente permissão]	Concede permissão para recuperar informações sobre a definição de preço do Amazon Detective	Read			
GetUsageInformation [somente permissão]	Concede permissão para listar informações de uso de um gráfico de comportamento	Leitura	Graph*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
InvokeAssistant [somente permissão]	Concede permissão para invocar o assistente de detetive	Leitura	Graph*		
ListDatasourcePackages	Concede permissão para listar os estados de ingestão do pacote de fonte de dados do grafo e os carimbos de data e hora das alterações de estado mais recentes em um grafo de comportamento gerenciado por essa conta	Lista	Graph*		
ListGraphs	Concede permissão para listar gráficos de comportamento gerenciados por essa conta	Lista			
ListHighDegreeEntities [somente permissão]	Concede permissão para recuperar entidades de alto volume cujos relacionamentos não possam ser armazenados pelo Detective	Lista	Graph*		
ListIndicators	Concede permissão para listar os indicadores de uma investigação	Lista	Graph*		
ListInvestigations	Concede permissão para listar as investigações de um gráfico de comportamento	Lista	Graph*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListInvitations	Concede permissão para recuperar detalhes sobre os gráficos de comportamento aos quais essa conta foi convidada a participar	List			
ListMembers	Concede permissão para recuperar detalhes de todos os membros de um gráfico de comportamento	Lista	Graph*		
ListOrganizationAdminAccount	Concede permissão para visualizar a conta de administrador delegado atual do Amazon Detective de uma organização	Lista			organizations:DescribeOrganization
ListTagsForResource	Concede permissão para listar os valores da etiqueta atribuídos a um gráfico de comportamento	Lista	Graph*		
				aws:ResourceTag/${TagKey}	
RejectInvitation	Concede permissão para rejeitar um convite para se tornar membro de um gráfico de comportamento	Write	Graph*		
SearchGraph [somente permissão]	Concede permissão para pesquisar os dados armazenados em um gráfico de comportamento	Leitura	Graph*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartInvestigation	Concede permissão para iniciar investigações	Gravar	Graph*		
StartMonitoringMember	Concede permissão para iniciar a ingestão de dados para uma conta-membro que tenha o status ACCEPTED_BUT_DISABLED	Gravar	Graph*		
TagResource	Concede permissão para atribuir valores da etiqueta a um gráfico de comportamento	Marcação	Graph*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permissão para remover valores da etiqueta de um gráfico de comportamento	Tags	Graph*		
				aws:TagKeys	
UpdateDatasourcePackages	Concede permissão para habilitar ou desabilitar os pacotes de fonte de dados em um grafo de comportamento gerenciado por essa conta	Gravar	Graph*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateInvestigationState	Concede permissão para atualizar o status e os metadados de uma investigação	Gravar	Graph*		
UpdateOrganizationConfiguration	Concede permissão para atualizar a configuração atual relacionada à integração do Amazon Detective com Organizations AWS	Gravar	Graph*		organizations:DescribeOrganization

Tipos de recursos definidos pelo Amazon Detective

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
Graph	`arn:${Partition}:detective:${Region}:${Account}:graph:${ResourceId}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Detective

O Amazon Detective define as chaves de condição a seguir que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as

condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso especificando as etiquetas que são transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso especificando as etiquetas associadas ao recurso	String
aws:TagKeys	Filtra o acesso especificando as chaves de etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Device Farm

AWS O Device Farm (prefixo do serviço:`devicefarm`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Device Farm
- Tipos de recursos definidos pelo AWS Device Farm
- Chaves de condição do AWS Device Farm

Ações definidas pelo AWS Device Farm

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDevicePool	Concede permissão para criar um grupo de dispositivos em um projeto	Write	project*		
CreateInstanceProfile	Concede permissão para criar um perfil de instância de dispositivo	Write			
CreateNetworkProfile	Concede permissão para criar um perfil de rede em um projeto	Write	project*		
CreateProject	Concede permissão para criar um projeto para teste móvel	Gravar			ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateRemoteAccessSession	Concede permissão para iniciar uma sessão de acesso remoto a uma instância de dispositivo	Write	device*		
			project*		
			deviceinstance		
			upload		
CreateTestGridProject	Concede permissão para criar um projeto para testes de desktop	Write			ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole
CreateTestGridUrl	Concede permissão para gerar um novo pre-signed URL usado para acessar nosso serviço de grade de teste	Write	testgrid-project*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateUpload	Concede permissão para fazer upload de um novo arquivo ou aplicativo em um projeto	Write	project*		
CreateVPCEConfiguration	Concede permissão para criar uma configuração de endpoint da Amazon Virtual Private Cloud (VPC)	Write			
DeleteDevicePool	Concede permissão para excluir um grupo de dispositivos gerado pelo usuário	Write	devicepool*		
DeleteInstanceProfile	Concede permissão para excluir um perfil de instância gerado pelo usuário	Write	instanceprofile*		
DeleteNetworkProfile	Concede permissão para excluir um perfil de rede gerado pelo usuário	Write	networkprofile*		
DeleteProject	Concede permissão para excluir um projeto de teste móvel	Write	project*		
DeleteRemoteAccessSession	Concede permissão para excluir uma sessão de acesso remoto concluída e seus resultados	Write	session*		
DeleteRun	Concede permissão para excluir uma execução	Write	run*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteTestGridProject	Concede permissão para excluir um projeto de teste de desktop	Write	testgrid-project*		
DeleteUpload	Concede permissão para excluir um arquivo carregado pelo usuário	Write	upload*		
DeleteVPCEConfiguration	Concede permissão para excluir uma configuração de endpoint da Amazon Virtual Private Cloud (VPC)	Gravar	vpceconfiguration*		
GetAccountSettings	Concede permissão para recuperar o número de dispositivos and/or iOS e Android ilimitados comprados pela conta	Leitura			
GetDevice	Concede permissão para recuperar as informações de um tipo de dispositivo único	Read	device*		
GetDeviceInstance	Concede permissão para recuperar as informações de uma instância de dispositivo	Read	deviceinstance*		
GetDevicePool	Concede permissão para recuperar as informações de um grupo de dispositivos	Leitura	devicepool*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetDevicePoolCompatibility	Concede permissão para recuperar informações sobre a compatibilidade de um and/or aplicativo de teste com um pool de dispositivos	Leitura	devicepool*		
			upload		
GetInstanceProfile	Concede permissão para recuperar as informações de um perfil de instância	Read	instanceprofile*		
GetJob	Concede permissão para recuperar as informações de um trabalho	Read	job*		
GetNetworkProfile	Concede permissão para recuperar as informações de um perfil de rede	Leitura	networkprofile*		
GetOfferingStatus	Concede permissão para recuperar o status atual e o status futuro de todas as ofertas adquiridas por um Conta da AWS	Leitura			
GetProject	Concede permissão para recuperar informações sobre um projeto de teste móvel	Read	project*		
GetRemoteAccessSession	Concede permissão para recuperar o link de uma sessão de acesso remoto em execução	Read	session*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetRun	Concede permissão para recuperar as informações de uma execução	Read	run*		
GetSuite	Concede permissão para recuperar as informações de um conjunto de testes	Read	suite*		
GetTest	Concede permissão para recuperar as informações de um caso de teste	Read	test*		
GetTestGridProject	Concede permissão para recuperar informações sobre um projeto de teste de desktop	Read	testgrid-project*		
GetTestGridSession	Concede permissão para recuperar as informações de uma sessão de grade de teste	Read	testgrid-project		
			testgrid-session		
GetUpload	Concede permissão para recuperar as informações de um arquivo carregado	Read	upload*		
GetVPCEConfiguration	Concede permissão para recuperar as informações de uma configuração de endpoint da Amazon Virtual Private Cloud (VPC)	Read	vpceconfiguration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
InstallToRemoteAccessSession	Concede permissão para instalar um aplicativo em um dispositivo em uma sessão de acesso remoto	Write	session*		
			upload*		
ListArtifacts	Concede permissão para listar os artefatos em um projeto	List	job		
			run		
			suite		
			test		
ListDeviceInstances	Concede permissão para listar as informações de instâncias de dispositivo	List			
ListDevicePools	Concede permissão para listar as informações de grupos de dispositivo	List	project*		
ListDevices	Concede permissão para listar as informações de tipos de dispositivo únicos	List			
ListInstanceProfiles	Concede permissão para listar as informações de perfis de instância de dispositivo	List			
ListJobs	Concede permissão para listar as informações de trabalhos em uma execução	List	run*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListNetworkProfiles	Concede permissão para listar as informações de perfis de rede em um projeto	List	project*		
ListOfferingPromotions	Concede permissão para listar as promoções oferecidas	Lista			
ListOfferingTransactions	Concede permissão para listar todas as compras históricas, renovações e transações de renovação do sistema de um Conta da AWS	Lista			
ListOfferings	Concede permissão para listar produtos ou ofertas que o usuário pode gerenciar pela API	Lista			
ListProjects	Concede permissão para listar as informações dos projetos de teste móvel para um Conta da AWS	Lista			
ListRemoteAccessSessions	Concede permissão para listar as informações de uma sessão de acesso remoto em execução no momento	List	project*		
ListRuns	Concede permissão para listar as informações de execuções em um projeto	List	project*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListSamples	Concede permissão para listar as informações de amostras em um projeto	List	job*		
ListSuites	Concede permissão para listar as informações de conjuntos de testes em um trabalho	List	job*		
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Lista	device		
			deviceinstance		
			devicepool		
			instanceprofile		
			networkprofile		
			project		
			run		
			session		
			testgrid-project		
			testgrid-session		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			vpceconfiguration		
ListTestGridProjects	Concede permissão para listar as informações dos projetos de teste de desktop para um Conta da AWS	Lista			
ListTestGridSessionActions	Concede permissão para listar as ações da sessão executadas durante uma sessão de grade de teste	List	testgrid-session*		
ListTestGridSessionArtifacts	Concede permissão para listar os artefatos gerados por uma sessão de grade de teste	List	testgrid-session*		
ListTestGridSessions	Concede permissão para listar as sessões de um projeto de grade de teste	List	testgrid-project*		
ListTests	Concede permissão para listar as informações de testes em um conjunto de testes	List	suite*		
ListUniqueProblems	Concede permissão para listar as informações de problemas únicos em uma execução	List	run*		
ListUploads	Concede permissão para listar as informações de uploads em um projeto	List	project*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListVPCEConfigurations	Concede permissão para listar as informações de configurações de endpoint da Amazon Virtual Private Cloud (VPC)	Lista			
PurchaseOffering	Concede permissão para comprar ofertas para um Conta da AWS	Gravar			
RenewOffering	Concede permissão para definir a quantidade de dispositivos a serem renovados para uma oferta	Write			
ScheduleRun	Concede permissão para programar uma execução	Write	project*		
			devicepool		
			upload		
	CENÁRIO: Device Pool as filter		devicepool* project* upload		
	CENÁRIO: Device Selection Configuration as filter		project* upload		
StopJob	Concede permissão para encerrar um trabalho em execução	Write	job*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopRemoteAccessSession	Concede permissão para encerrar uma sessão de acesso remoto em execução	Write	session*		
StopRun	Concede permissão para encerrar uma execução de teste	Write	run*		
TagResource	Concede permissão para adicionar tags a um recurso	Marcação	device		
			deviceinstance		
			devicepool		
			instanceprofile		
			networkprofile		
			project		
			run		
			session		
			testgrid-project		
			testgrid-session		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			vpceconfiguration		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover etiquetas de um recurso	Marcação	device		
			deviceinstance		
			devicepool		
			instanceprofile		
			networkprofile		
			project		
			run		
			session		
			testgrid-project		
			testgrid-session		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			vpceconfiguration		
				aws:TagKeys	
UpdateDeviceInstance	Concede permissão para modificar uma instância de dispositivo existente	Write	deviceinstance*		
			instanceprofile		
UpdateDevicePool	Concede permissão para modificar um grupo de dispositivos existente	Write	devicepool*		
UpdateInstanceProfile	Concede permissão para modificar um perfil de instância existente	Write	instanceprofile*		
UpdateNetworkProfile	Concede permissão para modificar um perfil de rede existente	Write	networkprofile*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateProject	Concede permissão para modificar um projeto de teste móvel existente	Write	project*		ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateTestGridProject	Concede permissão para modificar um projeto de teste de desktop existente	Write	testgrid-project*		ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole
UpdateUpload	Concede permissão para modificar um upload existente	Write	upload*		
UpdateVPCEConfiguration	Concede permissão para modificar uma configuração de endpoint da Amazon Virtual Private Cloud (VPC) existente	Write	vpceconfiguration*		

Tipos de recursos definidos pelo AWS Device Farm

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves

são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS Device Farm

AWS O Device Farm define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base no conjunto de valores permitidos para cada uma das etiquetas	String
aws:ResourceTag/${TagKey}	Filtra ações com base no valor da etiqueta associada ao recurso	String
aws:TagKeys	Filtra ações com base na presença de etiquetas obrigatórias na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o Amazon DevOps Guru

O Amazon DevOps Guru (prefixo do serviço:`devops-guru`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon DevOps Guru
- Tipos de recursos definidos pelo Amazon DevOps Guru
- Chaves de condição para Amazon DevOps Guru

Ações definidas pelo Amazon DevOps Guru

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddNotificationChannel	Concede permissão para adicionar um canal de notificação ao DevOps Guru	Gravar	topic*		sns:GetTopicAttributes sns:SetTopicAttributes
DeleteInsight	Concede permissão para excluir insights especificados de sua conta	Gravar			
DescribeAccountHealth	Concede permissão para visualizar a integridade das operações em seu Conta da AWS	Leitura			
DescribeAccountOverview	Concede permissão para visualizar a integridade das operações dentro de um intervalo de tempo em seu Conta da AWS	Leitura			
DescribeAnomaly	Concede permissão para listar os detalhes de uma anomalia especificada	Leitura			
DescribeEventSourcesConfig	Concede permissão para recuperar detalhes sobre fontes de eventos para DevOps o Guru	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeFeedback	Concede permissão para visualizar os detalhes de feedback de um insight especificado	Read			
DescribeInsight	Concede permissão para listar os detalhes de um insight especificado	Leitura			
DescribeOrganizationHealth	Concede permissão para visualizar a integridade das operações em sua organização	Leitura			
DescribeOrganizationOverview	Concede permissão para visualizar a integridade das operações dentro de um intervalo de tempo em sua organização	Leitura			
DescribeOrganizationResourceCollectionHealth	Concede permissão para visualizar a integridade das operações de cada AWS CloudFormation pilha, AWS serviços ou contas especificados no DevOps Guru em sua organização	Leitura			
DescribeResourceCollectionHealth	Concede permissão para visualizar a integridade das operações de cada AWS CloudFormation pilha especificada no DevOps Guru	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeServiceIntegration	Concede permissão para visualizar o status de integração dos serviços que podem ser integrados ao DevOps Guru	Leitura			
GetCostEstimation	Concede permissão para listar estimativas de custo de recursos de serviço	Leitura			
GetResourceCollection	Concede permissão para listar AWS CloudFormation as pilhas que o DevOps Guru está configurado para usar	Leitura			
ListAnomaliesForInsight	Concede permissão para listar anomalias de um determinado insight em sua conta	Lista		devops-guru:ServiceNames	
ListAnomalousLogGroups	Concede permissão para listar anomalias de log de um determinado insight em sua conta	Lista			
ListEvents	Concede permissão para listar eventos de recursos que são avaliados pelo DevOps Guru	Lista			
ListInsights	Concede permissão para listar insights em sua conta	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListMonitoredResources	Concede permissão para listar recursos monitorados pelo DevOps Guru em sua conta	Lista			
ListNotificationChannels	Concede permissão para listar canais de notificação configurados para o DevOps Guru em sua conta	Lista			
ListOrganizationInsights	Concede permissão para listar insights em sua organização	Lista			
ListRecommendations	Concede permissão para listar as recomendações de um insight especificado	Lista			
PutFeedback	Concede permissão para enviar um feedback ao DevOps Guru	Gravar			
RemoveNotificationChannel	Concede permissão para remover um canal de notificação do DevOps Guru	Gravar	topic*		sns:GetTopicAttributes sns:SetTopicAttributes
SearchInsights	Concede permissão para pesquisar insights em sua conta	Lista		devops-guru:ServiceNames	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SearchOrganizationInsights	Concede permissão para buscar insights em sua organização	Lista			
StartCostEstimation	Concede permissão para iniciar a criação de uma estimativa do custo mensal	Leitura			
UpdateEventSourcesConfig	Concede permissão para atualizar uma fonte de eventos para o DevOps Guru	Gravar			
UpdateResourceCollection	Concede permissão para atualizar a lista de AWS CloudFormation pilhas que são usadas para especificar quais AWS recursos em sua conta são analisados pelo DevOps Guru	Gravar			
UpdateServiceIntegration	Concede permissão para ativar ou desativar um serviço que se integra ao Guru DevOps	Gravar			

Tipos de recursos definidos pelo Amazon DevOps Guru

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves

são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
topic	`arn:${Partition}:sns:${Region}:${Account}:${TopicName}`	

Chaves de condição para Amazon DevOps Guru

O Amazon DevOps Guru define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
devops-guru:ServiceNames	Filtra o acesso por API para restringir o acesso a determinados nomes AWS de serviços	ArrayOfString

Ações, recursos e chaves de condição para as Ferramentas de diagnóstico da AWS

AWS As ferramentas de diagnóstico (prefixo do serviço:`ts`) fornecem os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelas Ferramentas de diagnóstico da AWS
- Tipos de recursos definidos pelas Ferramentas de diagnóstico da AWS
- Chaves de condição para Ferramentas de diagnóstico da AWS

Ações definidas pelas Ferramentas de diagnóstico da AWS

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetExecution	Concede permissão para obter detalhes sobre a execução específica nas ferramentas AWS de diagnóstico	Leitura	execution*		
GetExecutionOutput	Concede permissão para obter detalhes sobre resultados de execução específicos nas ferramentas AWS de diagnóstico	Leitura	execution*		
GetTool	Concede permissão para obter detalhes sobre uma ferramenta específica nas ferramentas AWS de diagnóstico	Leitura	tool*		
ListExecutions	Concede permissão para listar todas as execuções disponíve	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	is nas ferramentas AWS de diagnóstico				
ListTagsForResource	Concede permissão para listar as tags de um recurso AWS de ferramentas de diagnóstico	Leitura	execution*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListTools	Concede permissão para listar todas as ferramentas disponíveis nas Ferramentas AWS de diagnóstico	Lista			
StartExecution	Concede permissão para iniciar um fluxo de trabalho de execução de uma ferramenta específica nas ferramentas AWS de diagnóstico	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
TagResource	Concede permissão para marcar um recurso AWS de ferramentas de diagnóstico	Tags	execution*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para desmarcar um recurso de ferramentas AWS de diagnóstico	Tags	execution *		
				aws:TagKeys	

Tipos de recursos definidos pelas Ferramentas de diagnóstico da AWS

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
execution	`arn:${Partition}:ts::${Account}:execution/${UserId}/${ToolId}/${ExecutionId}`	aws:ResourceTag/${TagKey}
tool	`arn:${Partition}:ts::aws:tool/${ToolId}`	

Chaves de condição para Ferramentas de diagnóstico da AWS

AWS As ferramentas de diagnóstico definem as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelo conjunto de valores permitido para cada uma das etiquetas	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelo valor-etiqueta associado ao recurso	String
aws:TagKeys	Filtra o acesso pela presença de etiquetas obrigatórias na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Direct Connect

AWS O Direct Connect (prefixo do serviço:`directconnect`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Direct Connect
- Tipos de recursos definidos pelo AWS Direct Connect
- Chaves de condição do AWS Direct Connect

Ações definidas pelo AWS Direct Connect

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando

usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptDirectConnectGatewayAssociationProposal	Concede permissão para aceitar uma solicitação de proposta para anexar um gateway privado virtual a um gateway Direct Connect	Gravar	dx-gateway*		
AllocateConnectionOnInterconnect	Concede permissão para criar uma conexão hospedada em uma interconexão	Gravar	dxcon*		
AllocateHostedConnection	Concede permissão para criar uma nova conexão hospedada entre a rede de um parceiro do AWS Direct Connect e um local específico do AWS Direct Connect	Gravar	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
AllocatePrivateVirtualInterface	Concede permissão para provisionar uma interface virtual privada para pertencer a outro cliente	Gravar	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AllocatePublicVirtualInterface	Concede permissão para provisionar uma interface virtual pública para pertencer a outro cliente	Gravar	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
AllocateTransitVirtualInterface	Concede permissão para provisionar uma interface virtual em trânsito para pertencer a outro cliente	Gravar	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
AssociateConnectionWithLag	Concede permissão para associar uma conexão com um LAG	Gravar	dxcon*		
			dxlag*		
AssociateHostedConnection	Concede permissão para associar uma conexão hospedada e suas interfaces virtuais a um link aggregation group (LAG - Grupo de agregação de link) ou interconexão	Gravar	dxcon*		
			dxcon		
			dxlag		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateMacSecKey	Concede permissão para associar um par MAC Security (MACsec) Connection Key Name (CKN) /Connectivity Association Key (CAK) a uma AWS conexão dedicada do Direct Connect	Gravar	dxcon		
			dxlag		
AssociateVirtualInterface	Concede permissão para associar uma interface virtual a um link aggregation group (LAG - grupo de agregação de link) ou conexão	Gravar	dxvif*		
			dxcon		
			dxlag		
ConfirmConnection	Concede permissão para confirmar a criação de uma conexão hospedada em uma interconexão	Gravar	dxcon*		
ConfirmCustomerAgreement	Concede permissão para confirmar os termos de acordo ao criar a conexão ou o link aggregation group (LAG - grupo de agregação de link)	Gravar			
ConfirmPrivateVirtualInterface	Concede permissão para aceitar a propriedade de uma interface virtual privada criada por outro cliente	Gravar	dxvif*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ConfirmPublicVirtualInterface	Concede permissão para aceitar a propriedade de uma interface virtual pública criada por outro cliente	Gravar	dxvif*		
ConfirmTransitVirtualInterface	Concede permissão para aceitar a propriedade de uma interface virtual em trânsito criada por outro cliente	Gravar	dxvif*		
CreateBGPPeer	Concede permissão para criar um par de BGP na interface virtual especificada	Gravar	dxvif*		
CreateConnection	Concede permissão para criar uma nova conexão entre a rede do cliente e um local específico do AWS Direct Connect	Gravar	dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDirectConnectGateway	Concede permissão para criar um gateway Direct Connect, que é um objeto intermediário que permite conectar um conjunto de interfaces virtuais e gateways privados virtuais	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDirectConnectGatewayAssociation	Concede permissão para criar uma associação entre um gateway Direct Connect e um gateway privado virtual	Gravar	dx-gateway*		
CreateDirectConnectGatewayAssociationProposal	Concede permissão para criar uma proposta para associar o gateway privado virtual especificado ao gateway Direct Connect especificado	Gravar	dx-gateway*		
CreateInterconnect	Concede permissão para criar uma nova interconexão entre a rede de um parceiro do AWS Direct Connect e um local específico do AWS Direct Connect	Gravar	dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLag	Concede permissão para criar um grupo de agregação de links (LAG) com o número especificado de conexões físicas agrupadas entre a rede do cliente e um local específico do Direct AWS Connect	Gravar	dxcon		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePrivateVirtualInterface	Concede permissão para criar uma nova interface virtual privada	Gravar	dxcon		
			dxlag		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePublicVirtualInterface	Concede permissão para criar uma nova interface virtual pública	Gravar	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTransitVirtualInterface	Concede permissão para criar uma nova interface virtual de trânsito	Gravar	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteBGPPeer	Concede permissão para excluir o par de BGP especificado na interface virtual especificada com o endereço e o ASN do cliente especificado	Gravar	dxvif*		
DeleteConnection	Concede permissão para excluir a conexão	Gravar	dxcon*		
DeleteDirectConnectGateway	Concede permissão para excluir o gateway Direct Connect especificado	Gravar	dx-gateway*		
DeleteDirectConnectGatewayAssociation	Concede permissão para excluir a associação entre o gateway Direct Connect especificado e o gateway privado virtual	Gravar	dx-gateway*		
DeleteDirectConnectGatewayAssociationProposal	Concede permissão para excluir a solicitação de proposta de associação entre o gateway Direct Connect especificado e o gateway privado virtual	Gravar			
DeleteInterconnect	Concede permissão para excluir a interconexão especificada	Gravar	dxcon*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteLag	Concede permissão para excluir o link aggregation group (LAG - grupo de agregação de link) especificado	Gravar	dxlag*		
DeleteVirtualInterface	Concede permissão para excluir uma interface virtual	Gravar	dxvif*		
DescribeConnectionLoa	Concede permissão para descrever a LOA-CFA de uma conexão	Leitura	dxcon*		
DescribeConnections	Concede permissão para descrever todos as conexões nesta região	Leitura	dxcon		
DescribeConnectionsOnInterconnect	Concede permissão para descrever uma lista de conexões que foram provisionadas na interconexão determinada	Leitura	dxcon*		
DescribeCustomerMetadata	Concede permissão para visualizar uma lista de contratos com clientes, juntamente com seu status assinado e se o cliente é um NNIPartner parceiro, NNIPartner V2 ou não	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeDirectConnectGatewayAssociationProposals	Concede permissão para descrever uma ou mais propostas de associação de conexão entre um gateway privado virtual e um gateway Direct Connect	Leitura	dx-gateway		
DescribeDirectConnectGatewayAssociations	Concede permissão para descrever as associações entre seus gateways Direct Connect e gateways privados virtuais	Leitura	dx-gateway		
DescribeDirectConnectGatewayAttachments	Concede permissão para descrever os anexos entre seus gateways Direct Connect e interfaces virtuais	Leitura	dx-gateway		
DescribeDirectConnectGateways	Concede permissão para descrever todos os gateways Direct Connect ou apenas o gateway Direct Connect especificado	Leitura	dx-gateway		
DescribeHostedConnections	Concede permissão para descrever as conexões hospedadas que foram provisionadas na interconexão especificada ou no link aggregation group (LAG - grupo de agregação de link)	Leitura	dxcon dxlag		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeInterconnectLoa	Concede permissão para descrever a LOA-CFA de uma interconexão	Leitura	dxcon*		
DescribeInterconnects	Concede permissão para descrever uma lista de interconexões pertencentes à Conta da AWS	Leitura	dxcon		
DescribeLags	Concede permissão para descreve todos os seus link aggregation groups (LAG - grupo de agregação de link) ou LAG especificado	Leitura	dxlag		
DescribeLoa	Concede permissão para descrever a LOA-CFA para um LAG de conexão, interconexão ou link aggregation group (LAG - grupo de agregação de link)	Leitura	dxcon dxlag		
DescribeLocations	Concede permissão para descrever a lista de locais do AWS Direct Connect na AWS região atual	Leitura			
DescribeRouterConfiguration	Concede permissão para descrever Detalhes sobre o roteador para uma interface virtual	Leitura	dxvif*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeTags	Concede permissão para descrever as tags associadas aos recursos específicos do AWS Direct Connect	Leitura	dx-gateway		
			dxcon		
			dxlag		
			dxvif		
DescribeVirtualGateways	Concede permissão para descrever uma lista de gateways privados virtuais de propriedade da Conta da AWS	Leitura			
DescribeVirtualInterfaces	Concede permissão para descrever todas as interfaces virtuais de um Conta da AWS	Leitura	dxcon		
			dxlag		
			dxvif		
DisassociateConnectionFromLag	Concede permissão para desassociar uma conexão de um link aggregation group (LAG - grupo de agregação de link)	Gravar	dxcon*		
			dxlag*		
DisassociateMacSecKey	Concede permissão para remover a associação entre uma chave de segurança MAC Security (MACsec) e uma conexão dedicada do AWS Direct Connect	Gravar	dxcon		
			dxlag		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListVirtualInterfaceTestHistory	Concede permissão para listar o histórico do teste de failover da interface virtual	Lista	dxvif*		
StartBgpFailoverTest	Concede permissão para iniciar o teste de failover da interface virtual que verifica se a configuração atende aos requisitos de resiliência colocando a sessão de emparelhamento BGP no estado DOWN. Depois, você pode enviar tráfego para verificar se não há interrupções	Gravar	dxvif*		
StopBgpFailoverTest	Concede permissão para interromper o teste de failover da interface virtual	Gravar	dxvif*		
TagResource	Concede permissão para adicionar as tags especificadas ao recurso AWS Direct Connect especificado. Cada recurso pode ter um máximo de 50 etiquetas	Tags	dx-gateway		
			dxcon		
			dxlag		
			dxvif		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover uma ou mais tags do recurso AWS Direct Connect especificado	Tags	dx-gateway		
			dxcon		
			dxlag		
			dxvif		
				aws:TagKeys	
UpdateConnection	Concede permissão para atualizar a configuração da conexão dedicada do AWS Direct Connect. Você pode atualizar os seguintes parâmetros para uma conexão: O nome da conexão ou O modo de criptografia MAC Security (MACsec) da conexão	Gravar	dxcon*		
UpdateDirectConnectGateway	Concede permissão para atualizar o nome de um gateway do Direct Connect	Gravar	dx-gateway*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateDirectConnectGatewayAssociation	Concede permissão para atualizar os atributos especificados da associação do gateway Direct Connect	Gravar			
UpdateLag	Concede permissão para atualizar os atributos do link aggregation group (LAG - grupo de agregação de link) especificado	Gravar	dxlag*		
UpdateVirtualInterfaceAttributes	Concede permissão para atualizar os atributos especificados da interface virtual privada especificada	Gravar	dxvif*		

Tipos de recursos definidos pelo AWS Direct Connect

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
dxcon	`arn:${Partition}:directconnect:${Region}:${Account}:dxcon/${ConnectionId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS Direct Connect

AWS O Direct Connect define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por ações com base na presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por ações com base nos pares de chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso por ações com base na presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Directory Service

AWS O Directory Service (prefixo do serviço:`ds`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Directory Service
- Tipos de recursos definidos pelo AWS Directory Service
- Chaves de condição do AWS Directory Service

Ações definidas pelo AWS Directory Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptSharedDirectory	Concede permissão para aceitar uma solicitação de compartilhamento de diretório enviada da conta do proprietário do diretório	Gravar	directory*		
AccessDSData [somente permissão]	Concede permissão para acessar dados do diretório usando a API de dados do Directory Service	Gerenciamento de permissões	directory*		
AddIpRoutes	Concede permissão para adicionar um bloco de	Gravar	directory*		ec2:AuthorizeSecur

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	endereços CIDR para encaminhar corretamente o tráfego de e para o Microsoft AD no Amazon Web Services				ityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:DescribeSecurityGroups

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddRegion	Concede permissão para adicionar ao diretório selecionado dois controladores de domínio na região especificada para o diretório especificado	Gravar	directory*		ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddTagsToResource	Concede permissão para adicionar ou substituir uma ou mais etiquetas do diretório especificado do Amazon Directory Services	Tags	directory*		ec2:CreateTags
				aws:RequestTag/${TagKey} aws:TagKeys	
AuthorizeApplication [somente permissão]	Concede permissão para autorizar uma inscrição para o seu Diretório AWS	Gravar	directory*		
CancelSchemaExtension	Concede permissão para cancelar uma extensão de esquema em andamento para um diretório do Microsoft AD	Gravar	directory*		
CheckAlias [somente permissão]	Concede permissão para verificar se o alias está disponível para uso	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ConnectDirectory	Concede permissão para criar um AD Connector para se conectar a um diretório on-premises	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAlias	Concede permissão para criar um alias para um diretório e atribuí-lo ao diretório	Gravar	directory*		
CreateComputer	Concede permissão para criar uma conta de computador no diretório especificado e ingressa o computador no diretório	Gravar	directory*		
CreateConditionalForwarder	Concede permissão para criar um encaminhador condicional associado ao seu diretório AWS	Gravar	directory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDirectory	Concede permissão para criar um diretório Simple AD	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateHybridAD	Concede permissão para criar um diretório híbrido do AD gerenciado	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DescribeVpcs iam:CreateServiceLinkedRole iam:GetRole secretsmanager:DescribeSecret secretsmanager:GetSecretValue ssm:GetCommandInvocation ssm:GetConnectionStatus ssm:ListCommands ssm:SendCommand

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateIdentityPool Directory [somente permissão]	Concede permissão para criar um IdentityPool diretório na AWS nuvem	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLog Subscription	Concede permissão para criar uma assinatura para encaminhar registros de segurança do controlador de domínio do Directory Service em tempo real para o grupo de CloudWatch registros especificado em seu Conta da AWS	Gravar	directory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateMicrosoftAD	Concede permissão para criar um Microsoft AD na AWS nuvem	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSnapshot	Concede permissão para criar um instantâneo de um diretório Simple AD ou Microsoft AD na nuvem AWS	Gravar	directory*		
CreateTrust	Concede permissão para iniciar a criação do AWS lado de uma relação de confiança entre um Microsoft AD na AWS nuvem e um domínio externo	Gravar	directory*		
DeleteADAssessment	Concede permissão para excluir uma avaliação de diretório	Gravar			
DeleteConditionalForwarder	Concede permissão para excluir um encaminhador condicional que foi configurado para seu diretório AWS	Gravar	directory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteDirectory	Concede permissão para excluir um AWS diretório do Directory Service	Gravar	directory*		ec2:DeleteNetworkInterface ec2:DeleteSecurityGroup ec2:DescribeNetworkInterfaces ec2:RevokeSecurityGroupEgress ec2:RevokeSecurityGroupIngress
DeleteLogSubscription	Concede permissão para excluir a assinatura de Log especificada	Gravar	directory*		
DeleteSnapshot	Concede permissão para excluir um diretório snapshot	Gravar	directory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteTrust	Concede permissão para excluir uma relação de confiança existente entre seu Microsoft AD na AWS nuvem e um domínio externo	Gravar	directory*		
DeregisterCertificate	Concede permissão para excluir do sistema o certificado que foi registrado para uma conexão LDAP segura	Gravar	directory*		
DeregisterEventTopic	Concede permissão para remover o diretório especificado como publicador para o tópico do SNS especificado	Gravar	directory*		
DescribeADAssessment	Concede permissão para descrever uma avaliação de diretório	Leitura			
DescribeCertificate	Concede permissão para exibir informações sobre o certificado registrado para uma conexão LDAP segura	Leitura	directory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeClientAuthenticationSettings	Concede permissão para recuperar informações sobre o tipo de autenticação de cliente para o diretório especificado, se o tipo for especificado. Se nenhum tipo for especificado, as informações sobre todos os tipos de autenticação do cliente compatíveis com o diretório especificado serão recuperadas. Atualmente, somente SmartCard é suportado	Leitura	directory*		
DescribeConditionalForwarders	Concede permissão para obter informações sobre os encaminhadores condicionais dessa conta	Leitura	directory*		
DescribeDirectories	Concede permissão para obter informações sobre os diretórios que pertencem a essa conta	Lista			
DescribeDirectoryDataAccess	Concede permissão para descrever o status da API de dados do Directory Service para o diretório especificado	Leitura	directory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeDomainControllers	Concede permissão para fornecer informações sobre todos os controladores de domínio em seu diretório	Leitura	directory*		
DescribeEventTopics	Concede permissão para obter informações sobre quais tópicos do SNS recebem mensagens de status do diretório especificado	Leitura	directory*		
DescribeHybridADUpdate	Concede permissão para descrever as atualizações de um diretório híbrido especificado	Leitura	directory*		
DescribeLDAPSSettings	Concede permissão para descrever o status da segurança LDAP do diretório especificado	Leitura	directory*		
DescribeRegions	Concede permissão para fornecer informações sobre as regiões configuradas para replicação multirregional	Leitura	directory*		
DescribeSettings	Concede permissão para recuperar informações sobre as configurações ajustáveis para o diretório especificado	Leitura	directory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeSharedDirectories	Concede permissão para devolver os diretórios compartilhados em sua conta	Leitura	directory*		
DescribeSnapshots	Concede permissão para obter informações sobre os snapshots de diretório que pertencem a essa conta	Leitura			
DescribeTrusts	Concede permissão para obter informações sobre as relações de confiança dessa conta	Leitura			
DescribeUpdateDirectory	Concede permissão para descrever as atualizações de um diretório para um determinado tipo de atualização	Leitura	directory*		
DisableClientAuthentication	Concede permissão para desabilitar métodos alternativos de autenticação de clientes do diretório especificado	Gravar	directory*		
DisableDirectoryDataAccess	Concede permissão para desabilitar a API de dados do Directory Service para o diretório especificado	Gravar	directory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisableLDAPS	Concede permissão para desativar chamadas seguras LDAP para o diretório especificado	Gravar	directory*		
DisableRadius	Concede permissão para desabilitar a autenticação multifator (MFA) com o servidor Remote Authentication Dial In User Service (RADIUS) para um diretório do AD Connector	Gravar	directory*		
DisableRoleAccess [somente permissão]	Concede permissão para desativar o AWS Management Console acesso à identidade em seu AWS Diretório	Gravar	directory*		
DisableSso	Concede permissão para desabilitar o Single Sign-On para um diretório	Gravar	directory*		
EnableClientAuthentication	Concede permissão para habilitar métodos alternativos de autenticação de clientes do diretório especificado	Gravar	directory*		
EnableDirectoryDataAccess	Concede permissão para habilitar a API de dados do Directory Service para o diretório especificado	Gravar	directory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
EnableLDAPS	Concede permissão para ativar o switch para o diretório específico para sempre usar chamadas seguras LDAP	Gravar	directory*		
EnableRadius	Concede permissão para habilitar a autenticação multifator (MFA) com o servidor Remote Authentication Dial In User Service (RADIUS) para um diretório do AD Connector	Gravar	directory*		
EnableRoleAccess [somente permissão]	Concede permissão para permitir o AWS Management Console acesso à identidade em seu AWS Diretório	Gravar	directory*		iam:PassRole
EnableSso	Concede permissão para habilitar o single sign-on para um diretório	Gravar	directory*		
GetAuthorizedApplicationDetails [somente permissão]	Concede permissão para recuperar as informações das aplicações autorizadas em um diretório	Leitura	directory*		
GetDirectoryLimits	Concede permissão para obter informações sobre limites de diretório para a região atual	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSnapshotLimits	Concede permissão para obter os limites do snapshot manual de um diretório	Leitura	directory*		
ListADAssessments	Concede permissão para listar avaliações de diretórios	Lista			
ListAuthorizedApplications [somente permissão]	Concede permissão para obter os AWS aplicativos autorizados para um diretório	Leitura	directory*		
ListCertificates	Concede permissão para listar todos os certificados registrados para uma conexão LDAP segura para o diretório especificado	Lista	directory*		
ListIpRoutes	Concede permissão para listar os blocos de endereços que você adicionou a um diretório	Leitura	directory*		
ListLogSubscriptions	Concede permissão para listar as assinaturas de registro ativas do Conta da AWS	Leitura			
ListSchemaExtensions	Concede permissão para listar todas as extensões de esquema aplicadas a um diretório do Microsoft AD	Lista	directory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar todas as etiquetas em um diretório do Amazon Directory Services	Leitura	directory*		
RegisterCertificate	Concede permissão para registrar um certificado para conexão LDAP segura	Gravar	directory*		
RegisterEventTopic	Concede permissão para associar um diretório a um tópico do SNS	Gravar	directory*		sns:GetTopicAttributes
RejectSharedDirectory	Concede permissão para rejeitar uma solicitação de compartilhamento de diretório enviada da conta do proprietário do diretório	Gravar	directory*		
RemoveIpRoutes	Concede permissão para remover blocos de endereço IP de um diretório	Gravar	directory*		
RemoveRegion	Concede permissão para interromper toda a replicação e remover os controladores de domínio da região especificada. Não é possível remover a região principal com essa operação	Gravar	directory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RemoveTagsFromResource	Concede permissão para remover as etiquetas de um diretório do Amazon Directory Services	Tags	directory*		ec2:DeleteTags
				aws:RequestTag/${TagKey} aws:TagKeys	
ResetUserPassword	Concede permissão para redefinir a senha de qualquer usuário em seu diretório AWS Managed Microsoft AD ou Simple AD	Gravar	directory*		
RestoreFromSnapshot	Concede permissão para restaurar um diretório usando um snapshot existente do diretório	Gravar	directory*		
ShareDirectory	Concede permissão para compartilhar um diretório específico no seu Conta da AWS (proprietário do diretório) com outro Conta da AWS (consumidor do diretório). Com essa operação, você pode usar seu diretório de qualquer Conta da AWS e de qualquer Amazon VPC dentro de um Região da AWS	Gravar	directory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartADAssessment	Concede permissão para iniciar uma avaliação do diretório	Gravar			ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateSecurityGroup ec2:DeleteNetworkInterface ec2:DeleteSecurityGroup ec2:DescribeNetwor

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					kInterfaces ec2:DescribeSubnets ec2:DescribeVpcs ssm:GetCommandInvocation ssm:GetConnectionStatus ssm:ListCommands ssm:SendCommand
StartSchemaExtension	Concede permissão para aplicar uma extensão de esquema a um diretório do Microsoft AD	Gravar	directory*		
UnauthorizeApplication [somente permissão]	Concede permissão para desautorizar um aplicativo do seu Diretório AWS	Gravar	directory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UnshareDirectory	Concede a permissão de interromper o compartilhamento de diretório entre as contas proprietárias e consumidoras do diretório	Gravar	directory*		
UpdateAuthorizedApplication [somente permissão]	Concede permissão para atualizar um aplicativo autorizado para seu AWS Diretório	Gravar	directory*		
UpdateConditionalForwarder	Concede permissão para atualizar um encaminhador condicional que foi configurado para seu diretório AWS	Gravar	directory*		
UpdateDirectory [somente permissão]	Concede permissão para atualizar as configurações, como credenciais da conta de serviço ou endereços IP do servidor DNS para o diretório especificado	Gravar	directory*		
UpdateDirectorySetup	Concede permissão para atualizar o diretório para um tipo de atualização específico	Gravar	directory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateHybridAD	Concede permissão para atualizar as configurações de um diretório híbrido especificado	Gravar	directory*		ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DescribeVpcs secretsmanager:DescribeSecret secretsmanager:GetSecretValue ssm:GetCommandInvocation ssm:GetConnectionStatus ssm:ListCommands ssm:SendCommand

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateNumberOfDomainControllers	Concede a permissão de adicionar ou remover os controladores de domínio de ou para o diretório. Com base na diferença entre o valor atual e o novo valor (fornecidos por essa chamada de API), os controladores de domínio serão adicionados ou removidos. Pode levar até 45 minutos para que qualquer novo controlador de domínio se torne totalmente ativo depois que o número solicitado de controladores de domínio for atualizado. Durante esse período, não é possível fazer outra solicitação de atualização	Gravar	directory*		
UpdateRadius	Concede permissão para atualizar as informações do servidor Remote Authentication Dial In User Service (RADIUS) para um diretório do AD Connector	Gravar	directory*		
UpdateSettings	Concede permissão para atualizar as configurações ajustáveis para o diretório especificado	Gravar	directory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateTrust	Concede permissão para atualizar a relação de confiança que foi configurada entre seu diretório AWS gerenciado do Microsoft AD e um Active Directory local	Gravar	directory*		
VerifyTrust	Concede permissão para verificar uma relação de confiança entre seu Microsoft AD na AWS nuvem e um domínio externo	Leitura	directory*		

Tipos de recursos definidos pelo AWS Directory Service

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
directory	`arn:${Partition}:ds:${Region}:${Account}:directory/${DirectoryId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Directory Service

AWS O Directory Service define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelo valor da solicitação ao AWS DS	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelo recurso AWS DS que está sendo usado	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Directory Service Data

AWS O Directory Service Data (prefixo do serviço:`ds-data`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Directory Service Data

- Tipos de recursos definidos pelo AWS Directory Service Data
- Chaves de condição do AWS Directory Service Data

Ações definidas pelo AWS Directory Service Data

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddGroupMember	Concede permissão para adicionar um membro a um grupo de um diretório	Gravar	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:MemberNam ds-data:Realm ds-data:MemberRealm ds-data:Identifier	
CreateGroup	Concede permissão para criar um grupo em um diretório	Gravar	directory*		ds:AccessDSData
				ds-data:SAMAccountName	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ds-data:Identifier ds-data:Realm	
CreateUser	Concede permissão para criar um usuário em um diretório	Gravar	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
DeleteGroup	Concede permissão para excluir um grupo em um diretório	Gravar	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
DeleteUser	Concede permissão para excluir um usuário em um diretório	Gravar	directory*		ds:AccessDSData

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
DescribeGroup	Concede permissão para descrever um grupo em um diretório	Leitura	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
DescribeUser	Concede permissão para descrever um usuário no diretório	Leitura	directory*		ds:AccessDSData

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
DisableUser	Concede permissão para desabilitar um usuário em um diretório	Gravar	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
ListGroupMembers	Concede permissão para listar membros em um grupo de um diretório	Lista	directory*		ds:AccessDSData

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ds-data:SAMAccountName ds-data:Realm ds-data:MemberRealm ds-data:Identifier	
ListGroups	Concede permissão para listar os grupos em um diretório	Lista	directory*		ds:AccessDSData
				ds-data:Realm	
ListGroupsForMember	Concede permissão para listar os grupos dos quais um membro faz parte em um diretório	Lista	directory*		ds:AccessDSData

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ds-data:SAMAccountName ds-data:Realm ds-data:MemberRealm ds-data:Identifier	
ListUsers	Concede permissão para listar usuários em um diretório	Lista	directory*		ds:AccessDSData
				ds-data:Realm	
RemoveGroupMember	Concede permissão para remover um membro de um grupo em um diretório	Gravar	directory*		ds:AccessDSData

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ds-data:SAMAccountName ds-data:MemberNam ds-data:Realm ds-data:MemberRealm ds-data:Identifier	
SearchGroups	Concede permissão para pesquisar grupos em um diretório	Leitura	directory*		ds-data:DescribeGroup ds:AccessDSData
				ds-data:Realm	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SearchUsers	Concede permissão para pesquisar usuários em um diretório	Leitura	directory*		ds-data:DescribeUser ds:AccessDSData
				ds-data:Realm	
UpdateGroup	Concede permissão para atualizar um grupo em um diretório	Gravar	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
UpdateUser	Concede permissão para atualizar um usuário em um diretório	Gravar	directory*		ds:AccessDSData

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	

Tipos de recursos definidos pelo AWS Directory Service Data

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
directory	`arn:${Partition}:ds:${Region}:${Account}:directory/${DirectoryId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Directory Service Data

AWS O Directory Service Data define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso pelo recurso AWS DS que está sendo usado	String
ds-data:Identifier	Filtra o acesso pelo tipo de identificador fornecido na solicitação (ou seja, nome da conta do SAM)	String
ds-data:MemberName	Filtra o acesso pelo nome da conta do SAM do diretório incluído na MemberName entrada da solicitação	String
ds-data:MemberRealm	Filtra o acesso pelo nome da região do diretório incluído na MemberRealm entrada da solicitação	String
ds-data:Realm	Filtra o acesso pelo nome da região do diretório para a solicitação	String
ds-data:SAMAccountName	Filtra o acesso pelo nome da conta do SAM do diretório incluído na entrada SAMAccount Nome da solicitação	String

Ações, recursos e chaves de condição do Amazon DocumentDB Elastic Clusters

O Amazon DocumentDB Elastic Clusters (prefixo de serviço: `docdb-elastic`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon DocumentDB Elastic Clusters
- Tipos de recursos definidos pelo Amazon DocumentDB Elastic Clusters
- Chaves de condição do Amazon DocumentDB Elastic Clusters

Ações definidas pelo Amazon DocumentDB Elastic Clusters

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ApplyPendingMaintenanceAction	Concede permissão para aplicar ações de manutenção pendentes no cluster Amazon DocDB-Elastic	Gravar	cluster*		
				aws:ResourceTag/${TagKey}	
CopyClusterSnapshot	Concede permissão para copiar um novo snapshot de cluster do Amazon DocDB-Elastic	Gravar	cluster-snapshot*		docdb-elastic:CreateClusterSnapshot kms:CreateGrant kms:Decrypt kms:DescribeKey

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					kms:GenerateDataKey
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateCluster	Concede permissão para criar um novo cluster elástico do Amazon DocDB	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:ModifyVpcEndpoint iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey secretsmanager:DescribeSecret secretsmanager:GetResourcePolicy secretsmanager:Get

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					SecretValue secretsmanager:ListSecretVersionIds secretsmanager:ListSecrets

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateClusterSnapshot	Concede permissão para criar um novo snapshot de cluster elástico do Amazon DocDB	Gravar	cluster*		ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:ModifyVpcEndpoint iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey secretsmanager:DescribeSecret secretsmanager:GetResourcePolicy secretsmanager:Get

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					SecretValue secretsmanager:ListSecretVersionIds secretsmanager:ListSecrets
			cluster-snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteCluster	Concede permissão para excluir um cluster	Gravar	cluster*		ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteClusterSnapshot	Concede permissão para excluir um snapshot do cluster	Gravar	cluster-snapshot*		ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
GetCluster	Concede permissão para exibir detalhes sobre um cluster	Leitura	cluster*		
				aws:ResourceTag/${TagKey}	
GetClusterSnapshot	Concede permissão para exibir detalhes sobre um snapshot de cluster	Leitura	cluster-snapshot*		
				aws:ResourceTag/${TagKey}	
GetPendingMaintenanceAction	Concede permissão para visualizar detalhes sobre ações de manutenção pendentes no cluster Amazon DocDB-Elastic	Leitura	cluster*		
				aws:ResourceTag/${TagKey}	
ListClusterSnapshots	Concede permissão para listar os snapshots de cluster na sua conta	Lista			
ListClusters	Concede permissão para listar os clusters na sua conta	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListPendingMaintenanceActions	Concede permissão para listar detalhes sobre ações de manutenção pendentes em qualquer cluster Amazon DocDB-Elastic	Lista		aws:ResourceTag/${TagKey}	
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso do DocumentDB Elastic	Lista	cluster		
			cluster-snapshot		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RestoreClusterFromSnapshot	Concede permissão para restaurar um cluster de um snapshot de cluster elástico do Amazon DocDB	Gravar	cluster*		docdb-elastic:CreateCluster ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DescribeVpcs ec2:ModifyVpcEndpoint iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey secretsmanager:DescribeSecret secretsmanager:GetResourcePolicy

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					secretsmanager:GetSecretValue secretsmanager:ListSecretVersionIds secretsmanager:ListSecrets
			cluster-snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
StartCluster	Concede permissão para iniciar um cluster interrompido do Amazon DocDB-Elastic	Gravar	cluster*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopCluster	Concede permissão para interromper um cluster existente do Amazon DocDB-Elastic	Gravar	cluster*		
				aws:ResourceTag/${TagKey}	
TagResource	Concede permissão para etiquetar um recurso do DocumentDB Elastic	Tags	cluster		
			cluster-snapshot		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permissão para remover etiquetas de um recurso do DocumentDB Elastic	Tags	cluster		
			cluster-snapshot		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateCluster	Concede permissão para modificar um cluster	Gravar	cluster*		ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:ModifyVpcEndpoint kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey secretsmanager:DescribeSecret secretsmanager:GetResourcePolicy secretsmanager:GetSecretValue secretsmanager:Lis

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					tSecretVersionIds secretsmanager:ListSecrets
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pelo Amazon DocumentDB Elastic Clusters

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do Amazon DocumentDB Elastic Clusters

O Amazon DocumentDB Elastic Clusters define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelo conjunto de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelo conjunto de pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso pelo conjunto de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon DynamoDB

O Amazon DynamoDB (prefixo do serviço: `dynamodb`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon DynamoDB
- Tipos de recursos definidos pelo Amazon DynamoDB

- Chaves de condição do Amazon DynamoDB

Ações definidas pelo Amazon DynamoDB

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchGetItem	Concede permissão para retornar os atributos de um ou mais itens de uma ou mais tabelas	Leitura	table*		
				dynamodb:Attributes dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:Select	
BatchWriteItem	Concede permissão para adicionar ou excluir múltiplos itens em uma ou mais tabelas	Gravar	table*		
				dynamodb:Attributes dynamodb:LeadingKeys dynamodb:ReturnCon	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				sumedCapacity	
ConditionCheckItem	Concede permissão à ConditionCheckItem operação, verifica a existência de um conjunto de atributos para o item com a chave primária fornecida.	Leitura	table*		
				dynamodb:Attributes dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
CreateBackup	Concede permissão para criar um backup de uma tabela existente	Gravar	table*		
CreateGlobalTable	Concede permissão para criar uma tabela global a partir de uma tabela existente	Gravar	global-table*		
			table*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateGlobalTableWitness [somente permissão]	Concede permissão para adicionar uma testemunha a uma tabela global	Gravar	table*		
CreateTable	Concede permissão para a CreateTable operação, adiciona uma nova tabela à sua conta	Gravar	table*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTableReplica [somente permissão]	Concede permissão para adicionar uma nova tabela de réplica	Gravar	table*		
DeleteBackup	Concede permissão para excluir um backup existente de uma tabela	Gravar	backup*		
DeleteGlobalTableWitness [somente permissão]	Concede permissão para remover uma Testemunha de uma Tabela Global	Gravar	table*		
DeleteItem	Concede permissão para excluir um único item em uma tabela por chave primária	Gravar	table*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
DeleteResourcePolicy	Concede permissão para excluir a política baseada em recursos anexada ao recurso	Gerenciamento de permissões	stream* table*		
DeleteTable	Concede permissão à DeleteTable operação que exclui uma tabela e todos os seus itens	Gravar	table*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteTableReplica [somente permissão]	Concede permissão para excluir uma tabela de réplica e todos os seus itens	Gravar	table*		
DescribeBackup	Concede permissão para descrever um backup existente de uma tabela	Leitura	backup*		
DescribeContinuousBackups	Concede permissão para verificar o status das configurações de restauração do backup na tabela especificada	Leitura	table*		
DescribeContributorInsights	Concede permissão para descrever o status do contributor insights e os detalhes relacionados de determinada tabela ou índice secundário global	Leitura	table* index		
DescribeEndpoints	Concede permissão para retornar as informações de endpoint regional	Leitura			
DescribeExport	Concede permissão para descrever uma exportação de uma tabela existente	Leitura	export*		
DescribeGlobalTable	Concede permissão para retornar informações sobre o agente global especificado	Leitura	global-table*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeGlobalTableSettings	Concede permissão para retornar informações de configuração sobre o agente global especificado	Leitura	global-table*		
DescribeImport	Concede permissão para descrever uma importação existente	Leitura	import*		
DescribeKinesisStreamingDestination	Concede permissão para conceder permissão para descrever o status da transmissão do Kinesis e os detalhes relacionados de uma determinada tabela	Leitura	table*		
DescribeLimits	Concede permissão para retornar os limites atuais de capacidade provisionada para você Conta da AWS em uma região, tanto para a região como um todo quanto para qualquer tabela do DynamoDB que você criar lá	Leitura			
DescribeReservedCapacity [somente permissão]	Concede permissão para descrever uma ou mais da Capacidade Reservada adquirida	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeReservedCapacityOfferings [somente permissão]	Concede permissão para descrever as ofertas de Capacidade Reservada disponíveis para compra	Leitura			
DescribeStream	Concede permissão para retornar informações sobre uma transmissão, incluindo o status atual da transmissão, o nome do recurso da Amazon (ARN), a composição de seus estilhaços e sua tabela correspondente do DynamoDB	Leitura	stream*		
DescribeTable	Concede permissão para retornar informações sobre a tarefa	Leitura	table*		
DescribeTableReplicaAutoScaling	Concede permissão para descrever as configurações de Auto Scaling em todas as réplicas da tabela global	Leitura	table*		
DescribeTimeToLive	Concede permissão para fornecer uma descrição do status do tempo de vida (TTL) na tabela especificada	Leitura	table*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisableKinesisStreamingDestination	Concede permissão para conceder permissão para interromper a replicação da tabela do DynamoDB para o fluxo de dados do Kinesis	Gravar	table*		
EnableKinesisStreamingDestination	Concede permissão para conceder permissão para iniciar a replicação de dados de tabela para o fluxo de dados do Kinesis especificado em um carimbo de data/hora escolhido durante o fluxo de trabalho de habilitação	Gravar	table*		
ExportTableToPointInTime	Concede permissão para iniciar uma exportação de uma tabela do DynamoDB para o S3	Gravar	table*		
GetAbacStatus [somente permissão]	Concede permissão para visualizar o status do Controle de Acesso Baseado em Atributos da conta	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetItem	Concede permissão à GetItem operação que retorna um conjunto de atributos para o item com a chave primária fornecida	Leitura	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:Select	
GetRecords	Concede permissão para recuperar os registros da transmissão em um determina do fragmento	Leitura	stream*		
GetResourcePolicy	Concede permissão para exibir uma política baseada em recursos de um recurso	Leitura	stream*		
			table*		
GetShardIterator	Concede permissão para retornar um iterador de fragmento	Leitura	stream*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ImportTable	Concede permissão para iniciar uma importação do S3 para uma tabela do DynamoDB	Gravar	table*		
ListBackups	Concede permissão para listar os backups associados à conta e ao endpoint	Lista			
ListContributorInsights	Concede permissão para listar o ContributorInsightsSummary para todas as tabelas e índices secundários globais associados à conta atual e ao endpoint	Lista			
ListExports	Concede permissão para listar as exportações associadas à conta e ao endpoint	Lista			
ListGlobalTables	Concede permissão para listar todas as tabelas globais que têm uma réplica na região especificada	Lista			
ListImports	Concede permissão para listar as importações associadas à conta e ao endpoint	Lista			
ListStreams	Concede permissão para retornar uma matriz de fluxo ARNs associada à conta atual e ao endpoint	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTables	Concede permissão para retornar uma matriz de nomes de tabela associados à conta e ao endpoint atuais	Lista			
ListTagsOfResource	Concede permissão para listar todas as etiquetas em um recurso do Amazon DynamoDB	Leitura	table*		
PartiQLDelete	Concede permissão para excluir um único item em uma tabela por chave primária	Write	table*	dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnValues	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PartiQLInsert	Concede permissão para criar um novo item, se um item com a mesma chave primária não existir na tabela	Write	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys	
PartiQLSelect	Concede permissão para ler um conjunto de atributos para itens de uma tabela ou índice	Read	table*		
			index		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:FullTableScan dynamodb:LeadingKeys dynamodb:Select	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PartiQLUpdate	Concede permissão para editar os atributos de um item existente	Gravar	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnValues	
PurchaseReservedCapacityOfferings [somente permissão]	Concede permissão para comprar capacidade reservada para uso com sua conta	Gravar			
PutItem	Concede permissão para criar um novo item ou substituir um item antigo por um novo	Gravar	table*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
PutResourcePolicy	Concede permissão para anexar uma política baseada em recursos ao recurso	Gerenciamento de permissões	stream* table*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
Query	Concede permissão para usar a chave primária de uma tabela ou de um índice secundário para acessar diretamente os itens dessa tabela ou índice	Leitura	table*		
			index		
				dynamodb:Attributes dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues dynamodb:Select	
RestoreTableFromAwsBackup [somente permissão]	Concede permissão para criar uma nova tabela a partir do ponto de recuperação no AWS Backup	Gravar	table*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RestoreTableFromBackup	Concede permissão para criar uma nova tabela de um backup existente	Gravar	backup*		dynamodb:BatchWriteItem dynamodb:DeleteItem dynamodb:GetItem dynamodb:PutItem dynamodb:Query dynamodb:Scan dynamodb:UpdateItem
			table*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RestoreTableToPointInTime	Concede permissão para restaurar uma tabela para um momento	Gravar	table*		dynamodb:BatchWriteItem dynamodb:DeleteItem dynamodb:GetItem dynamodb:PutItem dynamodb:Query dynamodb:Scan dynamodb:UpdateItem
Scan	Concede permissão para retornar um ou mais itens e atributos de itens acessando cada item em uma tabela ou um índice secundário	Leitura	table*		
			index		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				dynamodb:Attributes dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues dynamodb:Select	
StartAwsBackupJob [somente permissão]	Concede permissão para criar um backup no AWS Backup com recursos avançados ativados	Gravar	table*		
TagResource	Concede permissão para associar um conjunto de etiquetas com um recurso do Amazon DynamoDB	Tags	table*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover a associação de etiquetas de um recurso do Amazon DynamoDB	Tags	table*		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateAbacStatus [somente permissão]	Concede permissão para atualizar o status do Controle de Acesso Baseado em Atributos para a conta	Gerenciamento de permissões			
UpdateContinuousBackups	Concede permissão para habilitar ou desabilitar backups contínuos	Gravar	table*		
UpdateContributorInsights	Concede permissão para atualizar o status do contributor insights para uma tabela ou índice secundário global específico	Gravar	table*		
			index		
UpdateGlobalTable	Concede permissão para adicionar ou remover réplicas na tabela global especificada	Gravar	global-table*		
			table*		
UpdateGlobalTableSettings	Concede permissão para atualizar configurações do conjunto de tarefas especificado	Gravar	global-table*		
			table*		
UpdateGlobalTableVersion [somente permissão]	Concede permissão para atualizar a versão da tabela global especificada	Gravar	global-table*		
			table		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateItem	Concede permissão para editar os atributos de um item existente, ou adiciona um novo item à tabela, se ele ainda não existir	Gravar	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
UpdateKinesisStreamingDestination	Concede permissão para atualizar configurações de replicação de dados para o fluxo de dados do Kinesis especificado	Gravar	table*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateTable	Concede permissão para modificar as configurações de throughput provisionada, índices secundários globais ou as configurações do DynamoDB Streams para uma determinada tabela	Gravar	table*		
UpdateTableReplicaAutoScaling	Concede permissão para atualizar as configurações de Auto Scaling na tabela-réplica	Gravar	table*		
UpdateTimeToLive	Concede permissão para habilitar ou desabilitar o TTL para a tabela especificada	Gravar	table*		

Tipos de recursos definidos pelo Amazon DynamoDB

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
index	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/index/${IndexName}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
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}`	

Chaves de condição do Amazon DynamoDB

O Amazon DynamoDB define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

> **Note**
>
> Para obter informações sobre como usar chaves de contexto para refinar o acesso ao DynamoDB usando uma política do IAM, consulte Uso de condições de política do IAM para controle de acesso refinado no Guia do desenvolvedor do Amazon DynamoDB.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString
dynamodb:Attributes	Filtra o acesso por nomes dos atributos (campo ou coluna) da tabela	ArrayOfString
dynamodb:EnclosingOperation	Filtra o acesso bloqueando APIs chamadas de transações e permite APIs chamadas sem transação e vice-versa	String
dynamodb:FullTableScan	Filtra o acesso ao bloquear a verificação completa da tabela	Bool
dynamodb:LeadingKeys	Filtra o acesso pela chave de partição da tabela	ArrayOfString
dynamodb:ReturnConsumedCapacity	Filtra o acesso pelo ReturnConsumedCapacity parâmetro de uma solicitação. Contém "TOTAL" ou "NONE"	String

Chaves de condição	Descrição	Tipo
dynamodb:ReturnValues	Filtra o acesso pelo ReturnValues parâmetro da solicitação. Contém um dos seguintes: "ALL_OLD", "UPDATED_OLD", "ALL_NEW", "UPDATED_NEW" ou "NONE"	String
dynamodb:Select	Filtra o acesso pelo parâmetro Select de uma solicitação de consulta ou exame	String

Ações, recursos e chaves de condição do Amazon DynamoDB Accelerator (DAX)

O Amazon DynamoDB Accelerator (DAX) (prefixo do serviço: `dax`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon DynamoDB Accelerator (DAX)
- Tipos de recursos definidos pelo Amazon DynamoDB Accelerator (DAX)
- Chaves de condição do Amazon DynamoDB Accelerator (DAX)

Ações definidas pelo Amazon DynamoDB Accelerator (DAX)

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchGetItem	Concede permissão para retornar os atributos de um ou mais itens de uma ou mais tabelas	Leitura	application*		
BatchWriteItem	Concede permissão para adicionar ou excluir múltiplos itens em uma ou mais tabelas	Gravar	application*		
ConditionCheckItem	Concede permissão à ConditionCheckItem operação que verifica a existência de um conjunto de atributos para o item com a chave primária fornecida	Leitura	application*		
CreateCluster	Concede permissão para criar um cluster do DAX	Gravar	application*		dax:CreateParameterGroup dax:CreateSubnetGroup ec2:CreateNetworkInterface ec2:DeleteNetworkInterface

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:GetRole iam:PassRole
CreateParameterGroup	Concede permissão para criar um grupo de parâmetros	Gravar			
CreateSubnetGroup	Concede permissão para criar um grupo de sub-redes	Gravar			
DecreaseReplicationFactor	Concede permissão para remover um ou mais nós de um cluster do DAX	Gravar	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteCluster	Concede permissão para excluir um cluster do DAX provisionado anteriormente	Gravar	application*		
DeleteItem	Concede permissão para excluir um único item em uma tabela por chave primária	Gravar	application*		
				dax:EnclosingOperation	
DeleteParameterGroup	Concede permissão para excluir o grupo de parâmetros especificado	Gravar			
DeleteSubnetGroup	Concede permissão para excluir um grupo de sub-redes	Gravar			
DescribeClusters	Concede permissão para retornar informações sobre todos os clusters do DAX provisionados	Lista	application		
DescribeDefaultParameters	Concede permissão para retornar as informações sobre o parâmetro do sistema padrão para o DAX	Lista			
DescribeEvents	Concede permissões para retornar eventos relacionados a clusters e grupos de parâmetros do DAX	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeParameterGroups	Concede permissão para retornar uma lista de descrições de grupo de parâmetros	Lista			
DescribeParameters	Concede permissão para retornar a lista de parâmetros detalhada de um grupo de parâmetros específico	Leitura			
DescribeSubnetGroups	Concede permissão para retornar uma lista de descrições de grupo de sub-redes	Lista			
GetItem	Concede permissão à GetItem operação que retorna um conjunto de atributos para o item com a chave primária fornecida	Leitura	application*		
				dax:EnclosingOperation	
IncreaseReplicationFactor	Concede permissão para adicionar um ou mais nós a um cluster do DAX	Gravar	application*		
ListTags	Concede permissão para retornar uma lista de todas as etiquetas para um cluster do DAX	Leitura	application*		
PutItem	Concede permissão para criar um novo item ou substituir um item antigo por um novo	Gravar	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				dax:EnclosingOperation	
Query	Concede permissão para usar a chave primária de uma tabela ou de um índice secundário para acessar diretamente os itens dessa tabela ou índice	Leitura	application*		
RebootNode	Concede permissão para um único nó de um cluster do DAX	Gravar	application*		
Scan	Concede permissão para retornar um ou mais itens e atributos de itens acessando cada item em uma tabela ou um índice secundário	Leitura	application*		
TagResource	Concede permissão para associar um conjunto de etiquetas a um recurso do DAX	Tags	application*		
UntagResource	Concede permissão para remover a associação de etiquetas de um recurso do DAX	Tags	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateCluster	Concede permissão para modificar as configurações de um cluster do DAX	Gravar	application*		
UpdateItem	Concede permissão para editar os atributos de um item existente, ou adiciona um novo item à tabela, se ele ainda não existir	Gravar	application*		
				dax:EnclosingOperation	
UpdateParameterGroup	Concede permissão para modificar os parâmetros de um grupo de parâmetros	Gravar			
UpdateSubnetGroup	Concede permissão para modificar um grupo de sub-redes existente	Gravar			

Tipos de recursos definidos pelo Amazon DynamoDB Accelerator (DAX)

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
application	`arn:${Partition}:dax:${Region}:${Account}:cache/${ClusterName}`	

Chaves de condição do Amazon DynamoDB Accelerator (DAX)

O Amazon DynamoDB Accelerator (DAX) define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
dax:EnclosingOperation	Usado para bloquear APIs chamadas de transações e permitir chamadas sem transação e APIs vice-versa	String

Ações, recursos e chaves de condição para o Amazon EC2 Auto Scaling

O Amazon EC2 Auto Scaling (prefixo do serviço:`autoscaling`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon EC2 Auto Scaling
- Tipos de recursos definidos pelo Amazon EC2 Auto Scaling
- Chaves de condição para o Amazon EC2 Auto Scaling

Ações definidas pelo Amazon EC2 Auto Scaling

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de

recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AttachInstances	Concede permissão para anexar uma ou mais EC2 instâncias ao grupo de Auto Scaling especificado	Gravar	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
AttachLoadBalancerTargetGroups	Concede permissão para anexa um ou mais grupos de destino ao grupo de Auto Scaling especificado	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TargetGroupARNs	
AttachLoadBalancers	Concede permissão para anexar um ou mais balancead	Gravar	autoScalingGroup*	autoscaling:Resour	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	ores de carga ao grupo de Auto Scaling especificado.			ceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:LoadBalancerNames	
AttachTrafficSources	Concede permissão para anexar uma ou mais fontes de tráfego a um grupo do Auto Scaling	Gravar	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TrafficSourceIdentifiers	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchDeleteScheduledAction	Concede permissão para excluir as ações programadas especificadas	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
BatchPutScheduledUpdateGroupAction	Concede permissão para criar ou atualizar várias ações de escalabilidade programadas para um grupo de Auto Scaling.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
CancelInstanceRefresh	Concede permissão para cancelar uma operação de atualização de instância em andamento	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CompleteLifecycleAction	Concede permissão para concluir a ação de ciclo de vida do token ou instância especificados com o resultado especificado	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
CreateAutoScalingGroup	Concede permissão para criar um grupo de Auto Scaling com o nome e os atributos especificados	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	iam:CreateServiceLinkedRole iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				autoscaling:CapacityReservationIds autoscaling:CapacityReservationResourceGroupArns autoscaling:InstanceTypes autoscaling:LaunchConfigurationName autoscaling:LaunchTemplateVersionSpecified autoscaling:LoadBalancerNames	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				autoscaling:MaxSize autoscaling:MinSize autoscaling:TargetGroupARNs autoscaling:TrafficSourceIdentifiers autoscaling:VPCZoneIdentifiers aws:RequestTag/${TagKey} aws:TagKeys	
CreateLaunchConfiguration	Concede permissão para criar uma configuração de execução	Write	launchConfiguration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				autoscaling:ImageId autoscaling:InstanceType autoscaling:SpotPrice autoscaling:MetadataHttpTokens autoscaling:MetadataHttpPutResponseHopLimit autoscaling:MetadataHttpEndpoint	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateOrUpdateTags	Concede permissão para criar ou atualizar etiquetas para o grupo de Auto Scaling especificado.	Marcação	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAutoScalingGroup	Concede permissão para excluir o grupo de Auto Scaling especificado.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteLaunchConfiguration	Concede permissão para excluir a configuração de execução especificada	Write	launchConfiguration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteLifecycleHook	Concede permissão para excluir o gancho do ciclo de vida especificado	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteNotificationConfiguration	Concede permissão para excluir a notificação especificada	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeletePolicy	Concede permissão para excluir a política de Auto Scaling especificada	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteScheduledAction	Concede permissão para excluir a ação programada especificada	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteTags	Concede permissão para excluir as etiquetas especificadas	Marcação	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteWarmPool	Concede permissão para excluir o grupo de alta atividade associado ao grupo do Auto Scaling.	Gravar	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DescribeAccountLimits	Concede permissão para descrever os limites atuais de recursos do Auto Scaling para seu Conta da AWS	Lista			
DescribeAdjustmentTypes	Concede permissão para descrever os tipos de ajuste de política para uso com PutScalingPolicy	Lista			
DescribeAutoScalingGroups	Concede permissão para descrever um ou mais grupos de Auto Scaling. Se uma lista de nomes não for fornecida, a chamada descreverá todos os grupos de Auto Scaling	List			
DescribeAutoScalingInstances	Concede permissão para descrever uma ou mais instâncias de Auto Scaling Se uma lista não for fornecida, a chamada descreverá todas as instâncias	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeAutoScalingNotificationTypes	Concede permissão para descrever os tipos de notificação compatíveis com o Auto Scaling	List			
DescribeInstanceRefreshes	Concede permissão para descrever uma ou mais atualizações de instância para um grupo de Auto Scaling	List			
DescribeLaunchConfigurations	Concede permissão para descrever uma ou mais configurações de execução. Se você omitir a lista de nomes, a chamada descreverá todas as configurações de execução	List			
DescribeLifecycleHookTypes	Concede permissão para descrever os tipos disponíveis de ganchos de ciclo de vida	List			
DescribeLifecycleHooks	Concede permissão para descrever os ganchos de ciclo de vida do grupo de Auto Scaling especificado	List			
DescribeLoadBalancerTargetGroups	Concede permissão para descrever os grupos de destino do grupo de Auto Scaling especificado	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeLoadBalancers	Concede permissão para descrever os balanceadores de carga do grupo de Auto Scaling especificado	Lista			
DescribeMetricCollectionTypes	Concede permissão para descrever as CloudWatch métricas disponíveis para o Auto Scaling	Lista			
DescribeNotificationConfigurations	Concede permissão para descrever as ações de notificação associadas ao grupo de Auto Scaling especificado	List			
DescribePolicies	Concede permissão para descrever as políticas do grupo de Auto Scaling especificado	List			
DescribeScalingActivities	Concede permissão para descrever uma ou mais ações de escalabilidade para o grupo de Auto Scaling especificado	Lista			
DescribeScalingProcessTypes	Concede permissão para descrever os tipos de processo de escalabilidade para uso com ResumeProcesses e SuspendProcesses	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeScheduledActions	Concede permissão para descrever as ações programadas para o grupo de Auto Scaling que ainda não foram executadas	List			
DescribeTags	Concede permissão para descrever as etiquetas especificadas	Read			
DescribeTerminationPolicyTypes	Concede permissão para descrever as políticas de encerramento compatíveis com o Auto Scaling	Lista			
DescribeTrafficSources	Concede permissão para descrever os grupos de destino do grupo de Auto Scaling especificado	Lista			
DescribeWarmPool	Concede permissão para descrever o grupo de alta atividade associado ao grupo do Auto Scaling	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DetachInstances	Concede permissão para remover uma ou mais instâncias do grupo de Auto Scaling especificado	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DetachLoadBalancerTargetGroups	Concede permissão para desanexar um ou mais grupos de destino do grupo de Auto Scaling especificado	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TargetGroupARNs	
DetachLoadBalancers	Concede permissão para remover um ou mais balanceadores de carga do grupo de Auto Scaling especificado	Gravar	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				autoscaling:LoadBalancerNames	
DetachTrafficSources	Concede permissão para desassociar uma ou mais fontes de tráfego de um grupo do Auto Scaling	Gravar	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TrafficSourceIdentifiers	
DisableMetricsCollection	Concede permissão para desativar o monitoramento de métricas especificadas para o grupo de Auto Scaling especificado	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
EnableMetricsCollection	Concede permissão para ativar o monitoramento de métricas especificadas para o grupo de Auto Scaling especificado	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
EnterStandby	Concede permissão para mover as instâncias especificadas para o modo de espera	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
ExecutePolicy	Concede permissão para executar a política especificada	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ExitStandby	Concede permissão para mover as instâncias especificadas para fora do modo de espera	Gravar	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
GetPredictiveScalingForecast	Concede permissão para recuperar os dados de previsão de uma política de escalabilidade preditiva	Lista			
PutLifecycleHook	Concede permissão para criar ou atualizar um gancho de ciclo de vida para o grupo de Auto Scaling especificado	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutNotificationConfiguration	Concede permissão para configurar um grupo de Auto Scaling para enviar notificações quando ocorrem eventos especificados	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
PutScalingPolicy	Concede permissão para criar ou atualizar uma política de um grupo de Auto Scaling	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
PutScheduledUpdateGroupAction	Concede permissão para criar ou atualizar uma ação de escalabilidade programada para um grupo de Auto Scaling	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				autoscaling:MaxSize autoscaling:MinSize	
PutWarmPool	Concede permissão para criar ou atualizar o grupo de alta atividade associado ao grupo especificado do Auto Scaling.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
RecordLifecycleActionHeartbeat	Concede permissão para registrar uma pulsação para a ação de ciclo de vida associada ao token ou instância especificados	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ResumeProcesses	Concede permissão para retomar os processos suspensos especificados ou todos os processos suspensos do Auto Scaling do grupo de Auto Scaling especificado	Gravar	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
RollbackInstanceRefresh	Concede permissão para reverter uma operação de atualização de instância em andamento	Gravar	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
SetDesiredCapacity	Concede permissão para definir o tamanho do grupo de Auto Scaling especificado	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SetInstanceHealth	Concede permissão para exibir o status de integrida de das associações de uma instância especificada	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
SetInstanceProtection	Concede permissão para atualizar as configurações de proteção de instância das instâncias especificadas	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
StartInstanceRefresh	Concede permissão para iniciar uma nova operação de atualização de instância	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SuspendProcesses	Concede permissão para suspender os processos especificados ou todos os processos do Auto Scaling do grupo de Auto Scaling especificado	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
TerminateInstanceInAutoScalingGroup	Concede permissão para encerrar a instância especificada e, opcionalmente, ajusta o tamanho do grupo desejado	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
UpdateAutoScalingGroup	Concede permissão para atualizar a configuração do grupo de Auto Scaling especificado	Gravar	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				autoscaling:CapacityReservationIds autoscaling:CapacityReservationResourceGroupArns autoscaling:InstanceTypes autoscaling:LaunchConfigurationName autoscaling:LaunchTemplateVersionSpecified autoscaling:MaxSize	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				autoscaling:MinSize autoscaling:VPCZoneIdentifiers	

Tipos de recursos definidos pelo Amazon EC2 Auto Scaling

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}`	

Chaves de condição para o Amazon EC2 Auto Scaling

O Amazon EC2 Auto Scaling define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
autoscaling:CapacityReservationIds	Filtra o acesso com base na reserva de capacidade IDs	ArrayOfString
autoscaling:CapacityReservationResourceGroupArns	Filtra o acesso com base no ARN de um grupo de recursos de reserva de capacidade	ArrayOfString
autoscaling:ImageId	Filtra o acesso com base no ID da AMI para a configuração de execução	String
autoscaling:InstanceType	Filtra o acesso com base no tipo de instância para a configuração de execução	String
autoscaling:InstanceTypes	Filtra o acesso com base nos tipos de instância presentes como substituições em um modelo de execução para uma política de instâncias mistas. Use-o para qualificar quais tipos de instância podem ser definidos explicitamente na política	String
autoscaling:LaunchConfigurationName	Filtra o acesso com base no nome de uma configuração de execução	String

Chaves de condição	Descrição	Tipo
autoscaling:LaunchTemplateVersionSpecified	Filtra o acesso considerando se os usuários podem especificar qualquer versão de um modelo de execução ou somente a versão mais recente ou padrão	Bool
autoscaling:LoadBalancerNames	Filtra o acesso com base no nome do balanceador de carga	ArrayOfString
autoscaling:MaxSize	Filtra o acesso com base no tamanho máximo de escalabilidade na solicitação	Numérico
autoscaling:MetadataHttpEndpoint	Filtra o acesso considerando se o endpoint HTTP estiver habilitado para o serviço de metadados da instância	String
autoscaling:MetadataHttpPutResponseHopLimit	Filtra o acesso com base no número permitido de saltos ao chamar o serviço de metadados da instância	Numeric
autoscaling:MetadataHttpTokens	Filtra o acesso considerando se os tokens são necessários ao chamar o serviço de metadados da instância (opcional ou obrigatório)	String
autoscaling:MinSize	Filtra o acesso com base no tamanho mínimo de escalabilidade na solicitação	Numérico
autoscaling:ResourceTag/${TagKey}	Filtra as ações com base nas etiquetas associadas ao recurso	String
autoscaling:SpotPrice	Filtra o acesso com base no preço das instâncias spot para a configuração de execução	Numérico

Chaves de condição	Descrição	Tipo
autoscaling:TargetGroupARNs	Filtra o acesso com base no ARN de um grupo de destino	ArrayOfARN
autoscaling:TrafficSourceIdentifiers	Filtra o acesso com base nos identificadores das fontes de tráfego	ArrayOfString
autoscaling:VPCZoneIdentifiers	Filtra o acesso com base no identificador de uma zona da VPC	ArrayOfString
aws:RequestTag/${TagKey}	Filtra ações com base nas etiquetas transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra as ações com base nas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra ações com base nas chaves da etiqueta transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o Amazon EC2 Image Builder

O Amazon EC2 Image Builder (prefixo do serviço:`imagebuilder`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon EC2 Image Builder
- Tipos de recursos definidos pelo Amazon EC2 Image Builder
- Chaves de condição para o Amazon EC2 Image Builder

Ações definidas pelo Amazon EC2 Image Builder

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelImageCreation	Concede permissão para cancelar a criação de uma imagem	Gravar	image*		
CancelLifecycleExecution	Concede permissão para cancelar a execução de um ciclo de vida	Gravar	lifecycleExecution*		
CreateComponent	Concede permissão para criar um novo componente	Write	component*		imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKe

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					yWithoutPlaintext s3:GetObject s3:ListBucket
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateContainerRecipe	Concede permissão para criar uma nova receita de contêiner	Write	containerRecipe*		ec2:DescribeImages ecr:DescribeImages ecr:DescribeRepositories imagebuilder:GetComponent imagebuilder:GetImage imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					s3:GetObject s3:ListBucket ssm:GetParameter
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDistributionConfiguration	Concede permissão para criar uma nova configuração de distribuição	Write	distributionConfiguration*		ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplates ec2:ModifyLaunchTemplate imagebuilder:TagResource s3:ListBucket ssm:GetParameter
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateImage	Concede permissão para criar uma nova imagem	Write	image*		ecr:BatchGetRepositoryScanningConfiguration ecr:DescribeRepositories iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe imagebuilder:GetIn

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					frastructureConfiguration imagebuilder:GetWorkflow imagebuilder:TagResource inspector2:BatchGetAccountStatus
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateImagePipeline	Concede permissão para criar um novo pipeline de imagem	Write	imagePipeline*		ecr:BatchGetRepositoryScanningConfiguration ecr:DescribeRepositories iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe imagebuilder:GetIn

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					frastructureConfiguration imagebuilder:GetWorkflow imagebuilder:TagResource inspector2:BatchGetAccountStatus
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateImageRecipe	Concede permissão para criar uma nova receita de imagem	Write	imageRecipe*		ec2:DescribeImages imagebuilder:GetComponent imagebuilder:GetImage imagebuilder:TagResource ssm:GetParameter
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateInfrastructureConfiguration	Concede permissão para criar uma nova configuração de infraestrutura	Gravar	infrastructureConfiguration*		ec2:DescribeAvailabilityZones ec2:DescribeHosts iam:PassRole imagebuilder:TagResource resource-groups:GetGroup sns:Publish

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys imagebuilder:CreatedResourceTagKeys imagebuilder:CreatedResourceTag/${TagKey} imagebuilder:Ec2MetadataHttpTokens imagebuilder:StatusTopicArn	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateLifecyclePolicy	Concede permissão para criar uma nova política de ciclo de vida	Gravar	lifecyclePolicy*		iam:PassRole imagebuilder:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys imagebuilder:LifecyclePolicyResourceType	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateWorkflow	Concede permissão para criar um novo fluxo de trabalho	Gravar	workflow*		imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext s3:GetObject s3:ListBucket
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteComponent	Concede permissão para excluir um componente	Write	component*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteContainerRecipe	Concede permissão para excluir uma receita de contêiner	Write	containerRecipe*		
DeleteDistributionConfiguration	Concede permissão para excluir a configuração de distribuição	Write	distributionConfiguration*		
DeleteImage	Concede permissão para excluir uma imagem	Write	image*		
DeleteImagePipeline	Concede permissão para excluir um pipeline de imagem	Write	imagePipeline*		
DeleteImageRecipe	Concede permissão para excluir uma receita de imagem	Write	imageRecipe*		
DeleteInfrastructureConfiguration	Concede permissão para excluir uma configuração de infraestrutura	Gravar	infrastructureConfiguration*		
DeleteLifecyclePolicy	Concede permissão para excluir uma política de ciclo de vida	Gravar	lifecyclePolicy*		
DeleteWorkflow	Concede permissão para excluir um fluxo de trabalho	Gravar	workflow*		
GetComponent	Concede permissão para visualizar detalhes sobre um componente	Read	component*		kms:Decrypt

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetComponentPolicy	Concede permissão para visualizar a política de recursos associada a um componente	Read	component*		
GetContainerRecipe	Concede permissão para visualizar detalhes sobre uma receita de contêiner	Read	containerRecipe*		
GetContainerRecipePolicy	Concede permissão para visualizar a política de recursos associada a uma receita de contêiner	Read	containerRecipe*		
GetDistributionConfiguration	Concede permissão para visualizar detalhes sobre uma configuração de distribuição	Read	distributionConfiguration*		
GetImage	Concede permissão para visualizar detalhes sobre uma imagem	Read	image*		
GetImagePipeline	Concede permissão para visualizar detalhes sobre um pipeline de imagem	Read	imagePipeline*		
GetImagePolicy	Concede permissão para visualizar a política de recursos associada a uma imagem	Read	image*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetImageRecipe	Concede permissão para visualizar detalhes sobre uma receita de imagem	Read	imageRecipe*		
GetImageRecipePolicy	Concede permissão para visualizar a política de recursos associada a uma receita de imagem	Read	imageRecipe*		
GetInfrastructureConfiguration	Concede permissão para visualizar detalhes sobre uma configuração de infraestrutura	Leitura	infrastructureConfiguration*		
GetLifecycleExecution	Concede permissão para visualizar detalhes sobre uma execução de ciclo de vida	Leitura	lifecycleExecution*		
GetLifecyclePolicy	Concede permissão para visualizar detalhes sobre uma política de ciclo de vida	Leitura	lifecyclePolicy*		
GetMarketplaceResource	Concede permissão para recuperar o recurso fornecido pelo Marketplace	Leitura	component*		
GetWorkflow	Concede permissão para visualizar detalhes sobre um fluxo de trabalho	Leitura	workflow*		kms:Decrypt
GetWorkflowExecution	Concede permissão para visualizar detalhes sobre a execução de um fluxo de trabalho	Leitura	workflowExecution*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetWorkflowStepExecution	Concede permissão para visualizar detalhes sobre a execução de uma etapa de fluxo de trabalho	Leitura	workflowStepExecution*		kms:Decrypt
ImportComponent	Concede permissão para importar um novo componente	Gravar	component*		imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext s3:GetObject s3:ListBucket
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ImportDiskImage	Concede permissão para importar uma imagem de disco	Gravar	imageVersion*		iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetInfrastructureConfiguration imagebuilder:GetWorkflow imagebuilder:TagResource s3:GetObject s3:ListBucket
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ImportVmImage	Concede permissão para importar uma imagem	Gravar	imageVersion*		ec2:DescribeImages ec2:DescribeImportImageTasks iam:CreateServiceLinkedRole imagebuilder:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
ListComponentBuildVersions	Concede permissão para listar as versões de compilação de componentes em sua conta	List	allComponentBuildVersions*		
ListComponents	Concede permissão para listar as versões de componentes pertencentes à sua conta ou compartilhadas com ela	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListContainerRecipes	Concede permissão para listar as receitas de contêiner pertencentes à sua conta ou compartilhadas com ela	List			
ListDistributionConfigurations	Concede permissão para listar as configurações de distribuição em sua conta	List			
ListImageBuildVersions	Concede permissão para listar as versões de compilação de imagem em sua conta	Lista	allImageBuildVersions*		
ListImagePackages	Concede permissão para retornar uma lista de pacotes instalados na imagem especificada	Lista	image*		
ListImagePipelineImages	Concede permissão para retornar uma lista de imagens criadas pelo pipeline especificado	Lista	imagePipeline*		
ListImagePipelines	Concede permissão para listar os pipelines de imagem em sua conta	List			
ListImageRecipes	Concede permissão para listar as receitas de imagem pertencentes à sua conta ou compartilhadas com ela	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListImageScanFindingAggregations	Concede permissão para listar as agregações às descobertas da verificação de imagem em sua conta	Lista	image		
			imagePipeline		
ListImageScanFindings	Concede permissão para listar as descobertas da verificação de imagem das imagens em sua conta	Lista	image		inspector2:ListFindings
			imagePipeline		
ListImages	Concede permissão para listar as versões de imagem pertencentes à sua conta ou compartilhadas com ela	List			
ListInfrastructureConfigurations	Concede permissão para listar as configurações de infraestrutura em sua conta	Lista			
ListLifecycleExecutionResources	Concede permissão para listar recursos para a execução de ciclo de vida especificada	Lista	lifecycleExecution*		
ListLifecycleExecutions	Concede permissão para listar execuções de ciclos de vida para o recurso especificado	Lista	image		
			lifecyclePolicy		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListLifecyclePolicies	Concede permissão para listar as políticas de ciclo de vida na sua conta	Lista			
ListTagsForResource	Concede permissão para listar etiquetas de um recurso do Image Builder	Leitura	component		
			containerRecipe		
			distributionConfiguration		
			image		
			imagePipeline		
			imageRecipe		
			infrastructureConfiguration		
			lifecyclePolicy		
			workflow		
ListWaitingWorkflowSteps	Concede permissão para listar as etapas do fluxo de trabalho em espera para a conta do chamador	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListWorkflowBuildVersions	Concede permissão para listar as versões de compilação de fluxo de trabalho em sua conta	Lista	allWorkflowBuildVersions*		
ListWorkflowExecutions	Concede permissão para listar as execuções de fluxo de trabalho da imagem especificada	Lista	image*		
ListWorkflowStepExecutions	Concede permissão para listar as execuções de etapas de fluxo de trabalho do fluxo de trabalho especificado	Lista	workflowExecution*		kms:Decrypt
ListWorkflows	Concede permissão para listar as versões de fluxo de trabalho pertencentes à sua conta ou compartilhadas com ela	Lista			
PutComponentPolicy	Concede permissão para definir a política de recursos associada a um componente	Permissions management	component*		
PutContainerRecipePolicy	Concede permissão para definir a política de recursos associada a uma receita de contêiner	Permissions management	containerRecipe*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutImagePolicy	Concede permissão para definir a política de recursos associada a uma imagem	Permissions management	image*		
PutImageRecipePolicy	Concede permissão para definir a política de recursos associada a uma receita de imagem	Gerenciamento de permissões	imageRecipe*		
SendWorkflowStepAction	Concede permissão para enviar uma ação para uma etapa do fluxo de trabalho	Gravar	image* workflowStepExecution*		
StartImagePipelineExecution	Concede permissão para criar uma nova imagem a partir de um pipeline	Gravar	imagePipeline*		iam:CreateServiceLinkedRole imagebuilder:GetImagePipeline
StartResourceStateUpdate	Concede permissão para iniciar uma atualização de estado para o recurso especificado	Gravar	image*		
TagResource	Concede permissão para marcar um recurso do Image Builder	Marcação	component containerRecipe		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			distributionConfiguration		
			image		
			imagePipeline		
			imageRecipe		
			infrastructureConfiguration		
			lifecyclePolicy		
			workflow		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para desmarcar um recurso do Image Builder	Marcação	component		
			containerRecipe		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			distributionConfiguration		
			image		
			imagePipeline		
			imageRecipe		
			infrastructureConfiguration		
			lifecyclePolicy		
			workflow		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateDistribution Configuration	Concede permissão para atualizar a configuração de distribuição existente	Write	distributionConfiguration*		ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplates ec2:ModifyLaunchTemplate s3:ListBucket ssm:GetParameter

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateImagePipeline	Concede permissão para atualizar um pipeline de imagem existente	Write	imagePipeline*		ecr:BatchGetRepositoryScanningConfiguration ecr:DescribeRepositories iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe imagebuilder:GetIn

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					frastructureConfiguration imagebuilder:GetWorkflow inspector2:BatchGetAccountStatus
UpdateInfrastructureConfiguration	Concede permissão para atualizar uma configuração de infraestrutura existente	Gravar	infrastructureConfiguration*		ec2:DescribeAvailabilityZones ec2:DescribeHosts iam:PassRole resource-groups:GetGroup sns:Publish

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				imagebuilder:CreatedResourceTagKeys imagebuilder:CreatedResourceTag/${TagKey} imagebuilder:Ec2MetadataHttpTokens imagebuilder:StatusTopicArn	
UpdateLifecyclePolicy	Concede permissão para atualizar uma política de ciclo de vida existente	Gravar	lifecyclePolicy*		iam:PassRole
				imagebuilder:LifecyclePolicyResourceType	

Tipos de recursos definidos pelo Amazon EC2 Image Builder

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
component	`arn:${Partition}:imagebuilder:${Region}:${Account}:component/${ComponentName}/${ComponentVersion}/${ComponentBuildVersion}`	aws:ResourceTag/${TagKey}
distributionConfiguration	`arn:${Partition}:imagebuilder:${Region}:${Account}:distribution-configuration/${DistributionConfigurationName}`	aws:ResourceTag/${TagKey}
image	`arn:${Partition}:imagebuilder:${Region}:${Account}:image/${ImageName}/${ImageVersion}/${ImageBuildVersion}`	aws:ResourceTag/${TagKey}
imageVersion	`arn:${Partition}:imagebuilder:${Region}:${Account}:image/${ImageName}/${ImageVersion}`	aws:ResourceTag/${TagKey}
imageRecipe	`arn:${Partition}:imagebuilder:${Region}:${Account}:image-recipe/${ImageRecipeName}/${ImageRecipeVersion}`	aws:ResourceTag/${TagKey}
containerRecipe	`arn:${Partition}:imagebuilder:${Region}:${Account}:container-recipe/${ContainerRecipeName}/${ContainerRecipeVersion}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
imagePipeline	arn:${Partition}:imagebuilder:${Region}:${Account}:image-pipeline/${ImagePipelineName}	aws:ResourceTag/${TagKey}
infrastructureConfiguration	arn:${Partition}:imagebuilder:${Region}:${Account}:infrastructure-configuration/${ResourceId}	aws:ResourceTag/${TagKey}
lifecycleExecution	arn:${Partition}:imagebuilder:${Region}:${Account}:lifecycle-execution/${LifecycleExecutionId}	
lifecyclePolicy	arn:${Partition}:imagebuilder:${Region}:${Account}:lifecycle-policy/${LifecyclePolicyName}	aws:ResourceTag/${TagKey}
workflow	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow/${WorkflowType}/${WorkflowName}/${WorkflowVersion}/${WorkflowBuildVersion}	aws:ResourceTag/${TagKey}
workflowExecution	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow-execution/${WorkflowExecutionId}	
workflowStepExecution	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow-step-execution/${WorkflowStepExecutionId}	
allComponentBuildVersions	arn:${Partition}:imagebuilder:${Region}:${Account}:component/${ComponentName}/${ComponentVersion}/*	

Tipos de recursos	ARN	Chaves de condição
allImageBuildVersions	`arn:${Partition}:imagebuilder:${Region}:${Account}:image/${ImageName}/${ImageVersion}/*`	
allWorkflowBuildVersions	`arn:${Partition}:imagebuilder:${Region}:${Account}:workflow/${WorkflowType}/${WorkflowName}/${WorkflowVersion}/*`	

Chaves de condição para o Amazon EC2 Image Builder

O Amazon EC2 Image Builder define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString
imagebuilder:Creat	Filtra o acesso pelos pares de chave-valor da etiqueta anexados ao recurso criado pelo Image Builder	String

Chaves de condição	Descrição	Tipo
edResourceTag/${TagKey}		
imagebuilder:CreatedResourceTagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString
imagebuilder:Ec2MetadataHttpTokens	Filtra o acesso pelo requisito de token HTTP de metadados da EC2 instância especificado na solicitação	String
imagebuilder:LifecyclePolicyResourceType	Filtra o acesso pelo tipo de recurso de política de ciclo de vida especificado na solicitação	String
imagebuilder:StatusTopicArn	Filtra o acesso pelo ARN do tópico do SNS na solicitação na qual as notificações de estado do terminal serão publicadas	ARN

Ações, recursos e chaves de condição para o Amazon EC2 Instance Connect

O Amazon EC2 Instance Connect (prefixo do serviço:`ec2-instance-connect`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon EC2 Instance Connect
- Tipos de recursos definidos pelo Amazon EC2 Instance Connect
- Chaves de condição para o Amazon EC2 Instance Connect

Ações definidas pelo Amazon EC2 Instance Connect

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
OpenTunnel	Concede permissão para estabelecer uma conexão SSH com uma EC2 EC2 instância usando o Instance Connect Endpoint	Gravar	instance-connect-endpoint*		
			instance-connect-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2-instance-connect:remotePort ec2-instance-connect:privat	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				elpAddress ec2-instance-connect:MaxTunnelDuration	
SendSSHPublicKey	Concede permissão para enviar uma chave pública SSH para a EC2 instância especificada para ser usada para SSH padrão	Gravar	instance*		
				ec2:osuser	
SendSerialConsoleSSHPublicKey	Concede permissão para enviar uma chave pública SSH para a EC2 instância especificada para ser usada para SSH do console serial	Gravar	instance*		

Tipos de recursos definidos pelo Amazon EC2 Instance Connect

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição para o Amazon EC2 Instance Connect

O Amazon EC2 Instance Connect define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	String
ec2-instance-connect:maxTunnelDuration	Filtra o acesso pela duração máxima da sessão associada à instância	Numérico

Chaves de condição	Descrição	Tipo
ec2-instance-connect:privateIpAddress	Filtra o acesso por endereço IP privado associado à instância	IPAddress
ec2-instance-connect:remotePort	Filtra o acesso pelo número de portas associado à instâncias	Numérico
ec2:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	String
ec2:osuser	Filtra o acesso especificando o nome de usuário padrão para a AMI usada para executar a instância	String

Ações, recursos e chaves de condição do Amazon EKS Auth

O Amazon EKS Auth (prefixo do serviço: `eks-auth`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon EKS Auth
- Tipos de recursos definidos pelo Amazon EKS Auth
- Chaves de condição do Amazon EKS Auth

Ações definidas pelo Amazon EKS Auth

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssumeRoleForPodIdentity	Concede permissão para trocar um token de conta de serviço do Kubernetes por credenciais temporárias AWS	Leitura	cluster*		

Tipos de recursos definidos pelo Amazon EKS Auth

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
cluster	`arn:${Partition}:eks:${Region}:${Account}:cluster/${ClusterName}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon EKS Auth

O Amazon EKS Auth define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso por uma chave da etiqueta e par de valores	String

Ações, recursos e chaves de condição do AWS Elastic Beanstalk

AWS O Elastic Beanstalk (`elasticbeanstalk`prefixo do serviço:) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Elastic Beanstalk
- Tipos de recursos definidos pelo AWS Elastic Beanstalk
- Chaves de condição do AWS Elastic Beanstalk

Ações definidas pelo AWS Elastic Beanstalk

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o

nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AbortEnvironmentUpdate	Concede permissão para cancelar a atualização da configuração de ambientes em	Gravar	environment*	elasticbeanstalk:I	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	andamento ou da implantação da versão da aplicação			nApplication	
AddTags	Concede permissão para adicionar etiquetas a um recurso do Elastic Beanstalk e para atualizar valores de etiquetas	Tags	application		
			applicationversion		
			configurationtemplate		
			environment		
			platform		
				aws:RequestTag/${TagKey} aws:TagKeys	
ApplyEnvironmentManagedAction	Concede permissão para aplicar uma ação gerenciada programada imediatamente	Gravar	environment*	elasticbeanstalk:InApplication	
AssociateEnvironmentOperationsRole	Concede permissão para associar uma função de operações a um ambiente	Gravar	environment*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CheckDNSAvailability	Concede permissão para conferir a disponibilidade do CNAME	Leitura			
ComposeEnvironments	Concede permissão para criar ou atualizar um grupo de ambientes, em que cada um executa um componente separado de uma única aplicação	Gravar	application*		
			applicationversion*	elasticbeanstalk:InApplication	
CreateApplication	Concede permissão para criar uma nova aplicação	Gravar	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateApplicationVersion	Concede permissão para criar uma versão da aplicação para uma aplicação	Gravar	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			applicationversion*	elasticbeanstalk:InApplication aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfigurationTemplate	Concede permissão para criar um modelo de configuração	Gravar	configurationtemplate*	elasticbeanstalk:InApplication	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				elasticbeanstalk:FromApplication elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromEnvironment elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironment	Concede permissão para iniciar um ambiente para uma aplicação	Gravar	environment*	elasticbeanstalk:InApplication	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform aws:RequestTag/${TagKey} aws:TagKeys	
CreatePlatformVersion	Concede permissão para criar uma nova versão de uma plataforma personalizada	Gravar	platform*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStorageLocation	Concede permissão para criar o local de armazenamento do Amazon S3 para a conta	Gravar			
DeleteApplication	Concede permissão para excluir uma aplicação juntamente com todas as versões e configurações associadas	Gravar	application*		
DeleteApplicationVersion	Concede permissão para excluir uma versão da aplicação de uma aplicação	Gravar	applicationversion*	elasticbeanstalk:InApplication	
DeleteConfigurationTemplate	Concede permissão para excluir um modelo de configuração	Gravar	configurationtemplate*	elasticbeanstalk:InApplication	
DeleteEnvironmentConfiguration	Concede permissão para excluir a configuração de rascunho associada ao ambiente em execução	Gravar	environment*	elasticbeanstalk:InApplication	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeletePlatformVersion	Concede permissão para excluir uma versão de uma plataforma personalizada	Gravar	platform*		
DescribeAccountAttributes	Concede permissão para recuperar uma lista de atributos de conta, incluindo cotas de recursos	Leitura			
DescribeApplicationVersions	Concede permissão para recuperar uma lista de versões de aplicativos armazenadas em um bucket de armazenamento do AWS Elastic Beanstalk	Lista	applicationversion	elasticbeanstalk:InApplication	
DescribeApplications	Concede permissão para recuperar as descrições de aplicações existentes	Lista	application		
DescribeConfigurationOptions	Concede permissão para recuperar as descrições de opções de configuração de ambientes	Leitura	configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	
			solutionstack		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeConfigurationSettings	Concede permissão para recuperar uma descrição das configurações de um conjunto de configurações	Leitura	configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	
DescribeEnvironmentHealth	Concede permissão para recuperar informações sobre a integridade geral de um ambiente	Leitura	environment		
DescribeEnvironmentManagedActionHistory	Concede permissão para recuperar uma lista de ações gerenciadas concluídas e com falha de um ambiente	Leitura	environment	elasticbeanstalk:InApplication	
DescribeEnvironmentManagedActions	Concede permissão para recuperar uma lista de ações gerenciadas futuras e em andamento de um ambiente	Leitura	environment	elasticbeanstalk:InApplication	
DescribeEnvironmentResources	Concede permissão para recuperar uma lista de AWS recursos para um ambiente	Leitura	environment	elasticbeanstalk:InApplication	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeEnvironments	Concede permissão para recuperar as descrições dos ambientes existentes	Lista	environment	elasticbeanstalk:InApplication	
DescribeEvents	Concede permissão para recuperar uma lista de descrições de eventos que correspondem a um conjunto de critérios	Leitura	application		
			applicationversion	elasticbeanstalk:InApplication	
			configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	
DescribeInstancesHealth	Concede permissão para recuperar informações mais detalhadas sobre a integrida de das instâncias do ambiente	Leitura	environment		
DescribePlatformVersion	Concede permissão para recuperar uma descrição de uma versão da plataforma gerenciada	Leitura	platform		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateEnvironmentOperationsRole	Concede permissão para desassociar uma função de operações a um ambiente	Gravar	environment*		
ListAvailableSolutionStacks	Concede permissão para recuperar uma lista dos nomes de pilhas de soluções disponíveis	Lista	solutionstack		
ListPlatformBranches	Concede permissão para recuperar uma lista das ramificações de plataforma disponíveis	Lista			
ListPlatformVersions	Concede permissão para recuperar uma lista das plataformas disponíveis	Lista	platform		
ListTagsForResource	Concede permissão para recuperar uma lista de etiquetas de um recurso do Elastic Beanstalk	Leitura	application		
			applicationversion		
			configurationtemplate		
			environment		
			platform		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutInstanceStatistics	Concede permissão para enviar estatísticas de instância para melhorar a integridade	Gravar	application*		
			environment*		
RebuildEnvironment	Concede permissão para excluir e recriar todos os AWS recursos de um ambiente e forçar uma reinicialização	Gravar	environment*	elasticbeanstalk:InApplication	
RemoveTags	Concede permissão para remover etiquetas de um recurso do Elastic Beanstalk	Tags	application		
			applicationversion		
			configurationtemplate		
			environment		
			platform		
				aws:TagKeys	
RequestEnvironmentInfo	Concede permissão para iniciar uma solicitação para compilar informações do ambiente implantado	Leitura	environment*	elasticbeanstalk:InApplication	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RestartAppServer	Concede permissão para solicitar um ambiente para reiniciar o servidor de contêiner de aplicativos em execução em cada EC2 instância da Amazon	Gravar	environment*	elasticbeanstalk:InApplication	
RetrieveEnvironmentInfo	Concede permissão para recuperar as informações compiladas de uma solicitação RequestEnvironmentInfo	Leitura	environment*	elasticbeanstalk:InApplication	
SwapEnvironmentCNAMEs	Concede permissão para trocar dois ambientes CNAMEs	Gravar	environment*	elasticbeanstalk:InApplication	
				elasticbeanstalk:FromEnvironment	
TerminateEnvironment	Concede permissão para terminar um ambiente	Gravar	environment*	elasticbeanstalk:InApplication	
UpdateApplication	Concede permissão para atualizar uma aplicação com propriedades especificadas	Gravar	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateApplicationResourceLifecycle	Concede permissão para atualizar a política de ciclo de vida de versão da aplicação associada à aplicação	Gravar	application*		
UpdateApplicationVersion	Concede permissão para atualizar uma versão da aplicação com propriedades especificadas	Gravar	applicationversion*	elasticbeanstalk:InApplication	
UpdateConfigurationTemplate	Concede permissão para atualizar um modelo de configuração com propriedades ou os valores de opções de configuração especificados	Gravar	configurationtemplate*	elasticbeanstalk:InApplication	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				elasticbeanstalk:FromApplication elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromEnvironment elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateEnvironment	Concede permissão para atualizar um ambiente	Gravar	environment*	elasticbeanstalk:InApplication	
				elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateTagsForResource	Não concede permissão para atualizar tags. Para conceder permissão para adicionar tags a um recurso do Elastic Beanstalk, remover tags e atualizar valores de tags, especifique elasticbeanstalk:e elasticbeanstalk: AddTags RemoveTags	Tags	application		
			applicationversion		
			configurationtemplate		
			environment		
			platform		
				aws:RequestTag/${TagKey} aws:TagKeys	
ValidateConfigurationSettings	Concede permissão para conferir a validação de um conjunto de definições de configuração para um ambiente ou modelo de configuração	Leitura	configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	

Tipos de recursos definidos pelo AWS Elastic Beanstalk

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
platform	`arn:${Partition}:elasticbeanstalk:${Region}::platform/${PlatformNameWithVersion}`	

Chaves de condição do AWS Elastic Beanstalk

AWS O Elastic Beanstalk define as seguintes chaves de condição que podem ser usadas `Condition` no elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base na presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra ações com base nos pares de chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações com base na presença de chaves da etiqueta na solicitação	ArrayOfString
elasticbeanstalk:FromApplication	Filtra o acesso por uma aplicação como uma dependência ou uma restrição em um parâmetro de entrada	ARN
elasticbeanstalk:FromApplicationVersion	Especifica o acesso por uma versão da aplicação como uma dependência ou uma restrição em um parâmetro de entrada	ARN

Chaves de condição	Descrição	Type
elasticbeanstalk:FromConfigurationTemplate	Filtra o acesso por um modelo de configuração como uma dependência ou uma restrição em um parâmetro de entrada	ARN
elasticbeanstalk:FromEnvironment	Filtra o acesso por um ambiente como uma dependência ou uma restrição em um parâmetro de entrada	ARN
elasticbeanstalk:FromPlatform	Filtra o acesso por uma plataforma como uma dependência ou uma restrição em um parâmetro de entrada	ARN
elasticbeanstalk:FromSolutionStack	Filtra o acesso por uma pilha de soluções como uma dependência ou uma restrição em um parâmetro de entrada	ARN
elasticbeanstalk:InApplication	Filtra o acesso pela aplicação que contém o recurso no qual a ação opera	ARN

Ações, recursos e chaves de condição do Amazon Elastic Block Store

O Amazon Elastic Block Store (prefixo de serviço: `ebs`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Elastic Block Store
- Tipos de recursos definidos pelo Amazon Elastic Block Store
- Chaves de condição do Amazon Elastic Block Store

Ações definidas pelo Amazon Elastic Block Store

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de

recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CompleteSnapshot	Concede permissão para selar e concluir o snapshot depois que todos os blocos de dados necessários foram gravados nele	Gravar	snapshot*		
				aws:ResourceTag/${TagKey}	
GetSnapshotBlock	Concede permissão para retornar os dados de um bloco em um snapshot do Amazon Elastic Block Store (EBS)	Leitura	snapshot*		
				aws:ResourceTag/${TagKey}	
ListChangedBlocks	Concede permissão para listar os blocos que são diferentes entre dois snapshots do Amazon Elastic Block Store (EBS) da mesma linhagem volume/snapshot	Leitura	snapshot*		
				aws:ResourceTag/${TagKey}	
ListSnapshotBlocks	Concede permissão para listar os blocos em um snapshot do Amazon Elastic Block Store (EBS)	Leitura	snapshot*		
				aws:ResourceTag/${TagKey}	
PutSnapshotBlock	Concede permissão para gravar um bloco de dados	Gravar	snapshot*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	em um snapshot criado pela operação StartSnapshot			aws:ResourceTag/${TagKey}	
StartSnapshot	Concede permissão para criar um snapshot do EBS	Gravar	snapshot		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ebs:Description ebs:ParentSnapshot ebs:VolumeSize	

Tipos de recursos definidos pelo Amazon Elastic Block Store

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves

são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
snapshot	`arn:${Partition}:ec2:${Region}::snapshot/${SnapshotId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ebs:Description ebs:ParentSnapshot ebs:VolumeSize

Chaves de condição do Amazon Elastic Block Store

O Amazon Elastic Block Store define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por um par de chave valor da etiqueta que é permitido na solicitação	Segmento

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso por um par de chave e valor da etiqueta de um recurso.	Segmento
aws:TagKeys	Filtra o acesso por uma lista de chaves da etiqueta que são permitidas na solicitação	ArrayOfString
ebs:Description	Filtra o acesso pela descrição do snapshot que está sendo criado	String
ebs:ParentSnapshot	Filtra o acesso pelo ARN do snapshot pai	ARN
ebs:VolumeSize	Filtra o acesso pelo tamanho do volume do snapshot que está sendo criado, em GiB	Numérico

Ações, recursos e chaves de condição do Amazon Elastic Container Registry

O Amazon Elastic Container Registry (prefixo do serviço: `ecr`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Elastic Container Registry
- Tipos de recursos definidos pelo Amazon Elastic Container Registry
- Chaves de condição do Amazon Elastic Container Registry

Ações definidas pelo Amazon Elastic Container Registry

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchCheckLayerAvailability	Concede permissão para verificar a disponibilidade de várias camadas de imagem em um registro e repositório especificados.	Read	repository*		
BatchDeleteImage	Concede permissão para excluir uma lista de imagens especificadas em um repositório especificado	Write	repository*		
BatchGetImage	Concede permissão para obter informações detalhadas das imagens especificadas dentro de um repositório especificado	Leitura	repository*		
BatchGetRepositoryScanningConfiguration	Concede permissão para recuperar a configuração de verificação de repositórios de uma lista de repositórios	Leitura	repository*		
BatchImportUpstreamImage [somente permissão]	Concede permissão para recuperar a imagem do registro upstream e importá-la para o registro privado	Gravar	repository*		
CompleteLayerUpload	Concede permissão para informar ao Amazon ECR que o upload da camada da	Gravar	repository*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	imagem para um registro, nome de repositório e ID de upload especificados foi concluído.				
CreatePullThroughCacheRule	Concede permissão para criar nova regra de cache de pull-through	Gravar			iam:CreateServiceLinkedRole
CreateRepository	Concede permissão para criar um repositório de imagens	Gravar	repository*		ecr:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateRepositoryCreationTemplate	Concede permissão para criar o modelo de criação do repositório	Gravar			ecr:CreateRepository ecr:PutLifecyclePolicy ecr:SetRepositoryPolicy iam:CreateServiceLinkedRole iam:PassRole
DeleteLifecyclePolicy	Concede permissão para excluir a política de ciclo de vida especificada	Gravar	repository*		
DeletePullThroughCacheRule	Concede permissão para excluir a regra de cache de pull-through	Gravar			
DeleteRegistryPolicy	Concede permissão para excluir a política de registro	Gerenciamento de permissões			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteRepository	Concede permissão para excluir um repositório de imagens existente	Gravar	repository*		
DeleteRepositoryCreationTemplate	Concede permissão para excluir o modelo de criação do repositório	Gravar			
DeleteRepositoryPolicy	Concede permissão para excluir a política do repositório de um repositório especificado	Gerenciamento de permissões	repository*		
DescribeImageReplicationStatus	Concede permissão para recuperar o status de replicação sobre uma imagem em um registro, incluindo o motivo da falha se a replicação falhar	Leitura	repository*		
DescribeImageScanFindings	Concede permissão para descrever as descobertas da verificação de imagem da imagem especificada	Read	repository*		
DescribeImages	Concede permissão para obter metadados sobre as imagens em um repositório incluindo o tamanho da imagem, as etiquetas da imagem e a data de criação.	Lista	repository*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribePullThroughCacheRules	Concede permissão para descrever as regras de cache de pull-through	Lista			
DescribeRegistry	Concede permissão para descrever as configurações de registro	Read			
DescribeRepositories	Concede permissão para descrever repositórios de imagens em um registro	Leitura	repository*		
DescribeRepositoryCreationTemplates	Concede permissão para descrever o modelo de criação do repositório	Leitura			
GetAccountSetting	Concede permissão para recuperar configurações da conta	Leitura		ecr:AccountSetting	
GetAuthorizationToken	Concede permissão para recuperar um token que é válido por 12 horas para um registro especificado	Read			
GetDownloadUrlForLayer	Concede permissão para recuperar o URL de download correspondente a uma camada de imagem	Leitura	repository*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetImageCopyStatus [somente permissão]	Concede permissão para recuperar o status de uma cópia de imagem	Leitura	repository*		
GetLifecyclePolicy	Concede permissão para recuperar a política de ciclo de vida especificada	Read	repository*		
GetLifecyclePolicyPreview	Concede permissão para recuperar os resultados da solicitação de visualização da política de ciclo de vida especificada	Read	repository*		
GetRegistryPolicy	Concede permissão para recuperar a política de registro	Leitura			
GetRegistryScanningConfiguration	Concede permissão para recuperar a configuração de varredura do registro	Leitura			
GetRepositoryPolicy	Concede permissão para recuperar a política de repositório de um repositório especificado	Read	repository*		
InitiateLayerUpload	Concede permissão para notificar o Amazon ECR de que você pretende fazer upload de uma camada de imagem	Gravar	repository*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListImages	Concede permissão para listar todas as imagens IDs de um determinado repositório	Lista	repository*		
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso do Amazon ECR	Leitura	repository*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutAccountSetting	Concede permissão para atualizar as configurações da conta	Gravar		ecr:AccountSetting	
PutImage	Concede permissão para criar ou atualizar o manifesto da imagem associado a uma imagem	Write	repository*		
PutImageScanningConfiguration	Concede permissão para atualizar a configuração de verificação de imagem para um repositório	Write	repository*		
PutImageTagMutability	Concede permissão para atualizar as configurações de mutabilidade da etiqueta de imagem de um repositório	Write	repository*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutLifecyclePolicy	Concede permissão para criar ou atualizar uma política de ciclo de vida	Write	repository*		
PutRegistryPolicy	Concede permissão para atualizar a política de registro	Gerenciamento de permissões			
PutRegistryScanningConfiguration	Concede permissão para atualizar a configuração de varredura de	Gravar			
PutReplicationConfiguration	Concede permissão para atualizar a configuração de replicação para o registro	Gravar			iam:CreateServiceLinkedRole
ReplicateImage [somente permissão]	Concede permissão para replicar imagens para o registro de destino	Write	repository*		
SetRepositoryPolicy	Concede permissão para aplicar uma política de repositório em um repositório especificado para controlar permissões de acesso	Permissions management	repository*		
StartImageScan	Concede permissão para iniciar uma verificação de imagem	Write	repository*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartLifecyclePolicyPreview	Concede permissão para iniciar uma visualização da política de ciclo de vida especificada	Write	repository*		
TagResource	Concede permissão para marcar um recurso do Amazon ECR	Marcação	repository*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso do Amazon ECR	Tags	repository*		
				aws:TagKeys	
UpdatePullThroughCacheRule	Concede permissão para atualizar a regra de cache de pull-through	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateRepositoryCreationTemplate	Concede permissão para atualizar o modelo de criação do repositório	Gravar			ecr:CreateRepository ecr:PutLifecyclePolicy ecr:SetRepositoryPolicy iam:CreateServiceLinkedRole iam:PassRole
UploadLayerPart	Concede permissão para fazer upload de uma parte da camada de imagem para o Amazon ECR	Gravar	repository*		
ValidatePullThroughCacheRule	Concede permissão para validar a regra de cache de pull-through	Leitura			

Tipos de recursos definidos pelo Amazon Elastic Container Registry

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso

também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
repository	`arn:${Partition}:ecr:${Region}:${Account}:repository/${RepositoryName}`	aws:ResourceTag/${TagKey} ecr:ResourceTag/${TagKey}

Chaves de condição do Amazon Elastic Container Registry

O Amazon Elastic Container Registry define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelo conjunto de valores permitido para cada uma das etiquetas	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelo valor-etiqueta associado ao recurso	String
aws:TagKeys	Filtra o acesso pela presença de etiquetas obrigatórias na solicitação	ArrayOfString
ecr:AccountSetting	Filtra o acesso pelo nome da configuração da conta ECR	String

Chaves de condição	Descrição	Tipo
ecr:ResourceTag/${TagKey}	Filtra o acesso pelo valor-etiqueta associado ao recurso	String

Ações, recursos e chaves de condição para o Amazon Elastic Container Registry Public

O Amazon Elastic Container Registry Public (prefixo de serviço: `ecr-public`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de IAM permissão.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Recursos definidos pelo Amazon Elastic Container Registry
- Tipos de recursos definidos pelo Amazon Elastic Container Registry Public
- Chaves de condição para o Amazon Elastic Container Registry

Recursos definidos pelo Amazon Elastic Container Registry

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchCheckLayerAvailability	Concede permissão para verificar a disponibilidade de várias camadas de imagem em um registro e repositório especificados.	Read	repository*		
BatchDeleteImage	Concede permissão para excluir uma lista de imagens especificadas em um repositório especificado	Write	repository*		
CompleteLayerUpload	Concede permissão para informar ao Amazon ECR que o upload da camada da imagem para um registro, nome de repositório e ID de upload especificados foi concluído.	Write	repository*		
CreateRepository	Concede permissão para criar um repositório de imagens	Write	repository*		ecr-public:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteRepository	Concede permissão para excluir um repositório de imagens existente	Write	repository*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteRepositoryPolicy	Concede permissão para excluir a política do repositório de um repositório especificado	Write	repository*		
DescribeImageTags	Concede permissão para descrever todas as etiquetas de imagem para um determinado repositório	List	repository*		
DescribeImages	Concede permissão para obter metadados sobre as imagens em um repositório incluindo o tamanho da imagem, as etiquetas da imagem e a data de criação.	Read	repository*		
DescribeRegistries	Concede permissão para recuperar os dados do catálogo associados a um registro	List	registry*		
DescribeRepositories	Concede permissão para descrever repositórios de imagens em um registro	List	repository		
GetAuthorizationToken	Concede permissão para recuperar um token que é válido por 12 horas para um registro especificado	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetRegistryCatalogData	Concede permissão para recuperar os dados do catálogo associados a um registro	Read	registry*		
GetRepositoryCatalogData	Concede permissão para recuperar os dados do catálogo associados a um repositório	Read	repository*		
GetRepositoryPolicy	Concede permissão para recuperar a política de repositório de um repositório especificado	Read	repository*		
InitiateLayerUpload	Concede permissão para notificar o Amazon ECR de que você pretende fazer upload de uma camada de imagem	Write	repository*		
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso do Amazon ECR	Read	repository*		
PutImage	Concede permissão para criar ou atualizar o manifesto da imagem associado a uma imagem	Write	repository*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutRegistryCatalogData	Concede permissão para criar e atualizar os dados do catálogo associados a um registro	Write	registry*		
PutRepositoryCatalogData	Concede permissão para atualizar os dados do catálogo associados a um repositório	Write	repository*		
SetRepositoryPolicy	Concede permissão para aplicar uma política de repositório em um repositório especificado para controlar permissões de acesso	Permissions management	repository*		
TagResource	Concede permissão para marcar um recurso do Amazon ECR	Marcação	repository*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso do Amazon ECR	Marcação	repository*		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UploadLayerPart	Concede permissão para fazer upload de uma parte da camada de imagem para o Amazon ECR Public	Write	repository*		

Tipos de recursos definidos pelo Amazon Elastic Container Registry Public

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
repository	`arn:${Partition}:ecr-public::${Account}:repository/${RepositoryName}`	aws:ResourceTag/${TagKey} ecr-public:ResourceTag/${TagKey}
registry	`arn:${Partition}:ecr-public::${Account}:registry/${RegistryId}`	

Chaves de condição para o Amazon Elastic Container Registry

O Amazon Elastic Container Registry Public define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar

ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra solicitações de criação com base no conjunto de valores permitidos para cada uma das etiquetas	String
aws:ResourceTag/${TagKey}	Filtra ações com base no etiqueta-value associado ao recurso	String
aws:TagKeys	Filtra solicitações de criação com base na presença de etiquetas obrigatórias na solicitação	ArrayOfString
ecr-public:ResourceTag/${TagKey}	Filtra ações com base no etiqueta-value associado ao recurso	String

Ações, recursos e chaves de condição do Amazon Elastic Container Service

O Amazon Elastic Container Service (prefixo do serviço: `ecs`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Elastic Container Service

- Tipos de recursos definidos pelo Amazon Elastic Container Service
- Chaves de condição do Amazon Elastic Container Service

Ações definidas pelo Amazon Elastic Container Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateCapacityProvider	Concede permissão para criar um provedor de capacidade. Os provedores de capacidade estão associados a um cluster do Amazon ECS e são usados em estratégias de provedor de capacidade para facilitar a autoescalabilidade do cluster.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCluster	Concede permissão para criar um cluster do Amazon ECS.	Write	cluster*	aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys ecs:capacity-provider ecs:fargate-epheme	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ral-storage-kms-key	
CreateService	Concede permissão para executar e manter o número desejado de tarefas a partir de uma definição de tarefa especificada pela criação do serviço.	Write	service*	ecs:cluster aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				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	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ecs:enable-ecs-managed-tags ecs:propagate-tags ecs:auto-assign-public-ip ecs:subnet ecs:task-cpu ecs:task-memory	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateTaskSet	Concede permissão para criar um conjunto de tarefas do Amazon ECS.	Write		aws:RequestTag/${TagKey} aws:TagKeys ecs:cluster ecs:capacity-provider ecs:service ecs:task-definition	
DeleteAccountSetting	Concede permissão para modificar o formato do ARN e do ID do recurso de um usuário ou uma função especificada do IAM ou do usuário raiz de uma conta. É possível especificar se o novo formato do ARN e do ID do recurso será desabilitado para recursos criados.	Write		ecs:account-setting	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteAttributes	Concede permissão para excluir um ou mais atributos personalizados de um recurso do Amazon ECS.	Write	container-instance*		
				aws:ResourceTag/${TagKey} ecs:cluster	
DeleteCapacityProvider	Concede permissão para excluir o provedor de capacidade especificado.	Write	capacity-provider*		
				aws:ResourceTag/${TagKey}	
DeleteCluster	Concede permissão para excluir o cluster especificado.	Write	cluster*	aws:ResourceTag/${TagKey}	
DeleteService	Concede permissão para excluir um serviço especificado de um cluster.	Gravar	service*		
				aws:ResourceTag/${TagKey} ecs:cluster	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteTaskDefinitions	Concede permissão para excluir as definições de tarefa especificadas pela família e pela revisão	Gravar	task-definition*		
				aws:ResourceTag/${TagKey}	
DeleteTaskSet	Concede permissão para excluir o conjunto de tarefas especificado.	Write	task-set*		
				aws:ResourceTag/${TagKey} ecs:cluster ecs:service	
DeregisterContainerInstance	Concede permissão para cancelar o registro de uma instância de contêiner do Amazon ECS do cluster especificado.	Write	cluster*	aws:ResourceTag/${TagKey}	
DeregisterTaskDefinition	Concede permissão para cancelar o registro da definição de tarefa especificada pela família e pela revisão.	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeCapacityProviders	Concede permissão para descrever um ou mais provedores de capacidade do Amazon ECS.	Read	capacity-provider*		
				aws:ResourceTag/${TagKey}	
DescribeClusters	Concede permissão para descrever um ou mais clusters.	Read	cluster*	aws:ResourceTag/${TagKey}	
DescribeContainerInstances	Concede permissão para descrever instâncias de contêiner do Amazon ECS.	Leitura	container-instance*		
				aws:ResourceTag/${TagKey} ecs:cluster	
DescribeServiceDeployments	Concede permissão para descrever uma ou mais de suas implantações de serviço	Leitura	service*	ecs:cluster aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			service-deployment*	ecs:cluster ecs:service aws:ResourceTag/${TagKey}	
DescribeServiceRevisions	Concede permissão para descrever uma ou mais de suas revisões de serviço	Leitura	service*	ecs:cluster aws:ResourceTag/${TagKey}	
			service-revision*	ecs:cluster ecs:service aws:ResourceTag/${TagKey}	
DescribeServices	Concede permissão para descrever os serviços especificados em execução no cluster.	Read	service*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} ecs:cluster	
DescribeTaskDefinition	Concede permissão para descrever uma definição de tarefa. Você pode especificar uma família e uma revisão para localizar informações sobre uma definição de tarefa específica ou simplesmente especificar a família para localizar a revisão ACTIVE (ATIVA) mais recente da família.	Read			
DescribeTaskSets	Concede permissão para descrever conjuntos de tarefas do Amazon ECS.	Read	task-set*		
				aws:ResourceTag/${TagKey} ecs:cluster ecs:service	
DescribeTasks	Concede permissão para descrever uma ou mais tarefas especificadas.	Read	task*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} ecs:cluster	
DiscoverPollEndpoint	Concede permissão para obter um endpoint do agente do Amazon ECS para pesquisar atualizações.	Write			
ExecuteCommand	Concede permissão para executar um comando remotamente em um contêiner do Amazon ECS.	Gravar	cluster* task*		
				aws:ResourceTag/${TagKey} ecs:cluster ecs:container-name ecs:task	
GetTaskProtection	Concede permissão para recuperar o status de proteção de tarefas em um serviço do Amazon ECS	Leitura	task*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} ecs:cluster	
ListAccountSettings	Concede permissão para listar as configurações da conta de um recurso do Amazon ECS para uma entidade principal especificada.	Read			
ListAttributes	Concede permissão para listar os atributos dos recursos do Amazon ECS dentro de um tipo de destino e cluster especificados.	List	cluster*	aws:ResourceTag/${TagKey}	
ListClusters	Concede permissão para obter uma lista dos clusters existentes.	List			
ListContainerInstances	Concede permissão para obter uma lista das instâncias de contêiner de um cluster especificado.	Lista	cluster*	aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListServiceDeployments	Concede permissão para obter uma lista de implantações de serviços para um serviço específico	Lista	service*	aws:ResourceTag/${TagKey} ecs:cluster	
ListServices	Concede permissão para obter uma lista dos serviços que estão sendo executados em um cluster especificado.	Lista		ecs:cluster	
ListServicesByNamespace	Concede permissão para obter uma lista de serviços que estão sendo executados em um namespace de Nuvem AWS mapa especificado	Lista		ecs:namespace	
ListTagsForResource	Concede permissão para obter uma lista das etiquetas do recurso especificado.	Read	capacity-provider		
			cluster		
			container-instance		
			service		
			task		
			task-definition		
			task-set		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
ListTaskDefinitionFamilies	Concede permissão para obter uma lista das famílias de definições de tarefa registradas na conta, o que pode incluir famílias que não têm mais definições ACTIVE (ATIVAS).	List			
ListTaskDefinitions	Concede permissão para obter uma lista das definições de tarefa registradas na conta.	List			
ListTasks	Concede permissão para obter uma lista das tarefas de um cluster especificado.	List	container-instance*		
				aws:ResourceTag/${TagKey} ecs:cluster	
Poll [somente permissão]	Concede permissão a um agente para ele se conectar ao Amazon ECS para relatar status e obter comandos.	Write	container-instance*		
				ecs:cluster	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutAccountSetting	Concede permissão para modificar o formato do ARN e do ID do recurso de um usuário ou uma função especificada do IAM ou do usuário raiz de uma conta. É possível especificar se os novos formatos de ARN e ID de recurso estão habilitados para novos recursos criados. É necessário habilitar essa configuração para usar os novos recursos do Amazon ECS, como a marcação de recursos.	Write		ecs:account-setting	
PutAccountSettingDefault	Concede permissão para modificar o formato do ARN e do ID de um tipo de recurso para todos os usuários do IAM em uma conta para a qual nenhuma configuração de conta individual foi definida. É necessário habilitar essa configuração para usar os novos recursos do Amazon ECS, como a marcação de recursos.	Write		ecs:account-setting	
PutAttributes	Concede permissão para criar ou atualizar um atributo em um recurso do Amazon ECS.	Write	container-instance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} ecs:cluster	
PutClusterCapacityProviders	Concede permissão para modificar os provedores de capacidade disponíveis e a estratégia-padrão de provedor de capacidade de um cluster.	Gravar	cluster*	aws:ResourceTag/${TagKey}	
				ecs:capacity-provider	
RegisterContainerInstance	Concede permissão para registrar uma EC2 instância no cluster especificado	Gravar	cluster*	aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
RegisterTaskDefinition	Concede permissão para registrar uma nova definição de tarefa da família fornecida e do containerDefinitions.	Write	task-definition*	aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys ecs:compute-compatibility ecs:privileged ecs:task-cpu ecs:task-memory	
RunTask	Concede permissão para iniciar uma tarefa usando posicionamento aleatório e o programador-padrão do Amazon ECS.	Write	task-definition*		iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys ecs:cluster ecs:capacity-provider ecs:enable-ebs-volumes ecs:enable-execute-command	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartTask	Concede permissão para iniciar uma nova tarefa a partir da definição de tarefa especificada na instância ou instâncias de contêiner 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 permissão para iniciar uma sessão de telemetria.	Gravar	container-instance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ecs:cluster	
StopServiceDeployment	Concede permissão para interromper uma implantação de serviço em andamento	Gravar	service*	ecs:cluster aws:ResourceTag/${TagKey}	
			service-deployment*	ecs:cluster ecs:service aws:ResourceTag/${TagKey}	
StopTask	Concede permissão para interromper uma tarefa em execução.	Write	task*		
				aws:ResourceTag/${TagKey} ecs:cluster	
SubmitAttachmentStateChanges	Concede permissão para enviar uma confirmação de que os anexos mudaram de estado.	Write	cluster*	aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SubmitContainerStateChange	Concede permissão para enviar uma confirmação de que um contêiner mudou de estado.	Write	cluster*	aws:ResourceTag/${TagKey}	
SubmitTaskStateChange	Concede permissão para enviar uma confirmação de que uma tarefa mudou de estado.	Write	cluster*	aws:ResourceTag/${TagKey}	
TagResource	Concede permissão para marcar o recurso especificado	Marcação	capacity-provider		
			cluster		
			container-instance		
			service		
			task		
			task-definition		
			task-set		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} ecs:CreateAction	
UntagResource	Concede permissão para desmarcar o recurso especificado	Marcação	capacity-provider		
			cluster		
			container-instance		
			service		
			task		
			task-definition		
			task-set		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCapacityProvider	Concede permissão para atualizar o provedor de capacidade especificado.	Write	capacity-provider*		
				aws:ResourceTag/${TagKey}	
UpdateCluster	Concede permissão para modificar a configuração ou as configurações a serem usadas em um cluster.	Write	cluster*	aws:ResourceTag/${TagKey}	
				ecs:fargate-ephemeral-storage-kms-key	
UpdateClusterSettings	Concede permissão para modificar as configurações a serem usadas em um cluster.	Write	cluster*	aws:ResourceTag/${TagKey}	
UpdateContainerAgent	Concede permissão para atualizar o agente de contêiner do Amazon ECS em uma instância de contêiner especificada.	Write	container-instance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} ecs:cluster	
UpdateContainerInstancesState	Concede ao usuário permissão para modificar o status de uma instância de contêiner do Amazon ECS.	Write	container-instance*		
				aws:ResourceTag/${TagKey} ecs:cluster	
UpdateService	Concede permissão para modificar os parâmetros de um serviço.	Write	service*	ecs:cluster aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				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	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ecs:propagate-tags ecs:auto-assign-public-ip ecs:subnet ecs:task-cpu ecs:task-memory	
UpdateServicePrimaryTaskSet	Concede permissão para modificar o conjunto de tarefas primário usado em um serviço.	Gravar	service*		
				aws:ResourceTag/${TagKey} ecs:cluster	
UpdateTaskProtection	Concede permissão para modificar o status de proteção de uma tarefa	Gravar	task*		
				aws:ResourceTag/${TagKey} ecs:cluster	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateTaskSet	Concede permissão para atualizar o conjunto de tarefas especificado.	Write	task-set*		
				aws:ResourceTag/${TagKey} ecs:cluster ecs:service	

Tipos de recursos definidos pelo Amazon Elastic Container Service

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
		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 recursos	ARN	Chaves de condição
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}

Chaves de condição do Amazon Elastic Container Service

O Amazon Elastic Container Service define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Chaves de condição	Descrição	Tipo
ecs:CreateAction	Filtra o acesso pelo nome de uma ação de API de criação de recurso	String
ecs:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
ecs:account-setting	Filtra o acesso com base no nome de configuração da conta do Amazon ECS	String
ecs:auto-assign-public-ip	Filtra o acesso pela configuração de atribuição de IP público de sua tarefa do Amazon ECS ou serviço do Amazon ECS que usa o modo de rede awsvpc	Bool
ecs:capacity-provider	Filtra o acesso pelo ARN de um provedor de capacidade do Amazon ECS	ArrayOfARN
ecs:cluster	Filtra o acesso pelo ARN de um cluster do Amazon ECS	ARN
ecs:compute-compatibility	Filtra o acesso pelo campo de compatibilidades obrigatório fornecido na solicitação	ArrayOfString
ecs:container-instances	Filtra o acesso pelo ARN de uma instância de contêiner do Amazon ECS	ARN
ecs:container-name	Filtra o acesso pelo nome de um contêiner do Amazon ECS especificado na definição de tarefa do ECS.	String
ecs:enable-ebs-volumes	Filtra o acesso pelo recurso de volume do Amazon EBS gerenciado pelo Amazon ECS da sua tarefa ou serviço do ECS	String
ecs:enable-ecs-managed-tags	Filtra o acesso pela configuração de habilitação de ECSManaged tags de sua tarefa do Amazon ECS ou serviço do Amazon ECS	Bool

Chaves de condição	Descrição	Tipo
ecs:enable-execute-command	Filtra o acesso pelo recurso execute-command da tarefa ou do serviço do Amazon ECS	String
ecs:enable-service-connect	Filtra o acesso pelo valor de campo de ativação na configuração do Service Connect	String
ecs:enable-vpc-lattice	Filtra o acesso pela capacidade de rede VPC do seu serviço Amazon ECS	String
ecs:fargate-ephemeral-storage-kms-key	Filtra o acesso pelo ID da chave AWS KMS fornecido na solicitação	String
ecs:namespace	Filtra o acesso pelo ARN do namespace Nuvem AWS Map, que é definido na Configuração do Service Connect	ARN
ecs:privileged	Filtra o acesso pelo campo privilegiado fornecido na solicitação	String
ecs:propagate-tags	Filtra o acesso pela configuração de propagação de tags de sua tarefa do Amazon ECS ou serviço do Amazon ECS	String
ecs:service	Filtra o acesso pelo ARN de um serviço do Amazon ECS	ARN
ecs:subnet	Filtra o acesso pela configuração de sub-rede da sua tarefa do Amazon ECS ou serviço do Amazon ECS que usa o modo de rede awsvpc	ArrayOfString
ecs:task	Filtra o acesso pelo ARN de uma tarefa do Amazon ECS	ARN
ecs:task-cpu	Filtra o acesso pela CPU da tarefa, como um número inteiro com 1024 = 1 vCPU, fornecido na solicitação	Numérico

Chaves de condição	Descrição	Tipo
ecs:task-definition	Filtra o acesso pelo ARN de uma definição de tarefa do Amazon ECS	ARN
ecs:task-memory	Filtra o acesso pela memória da tarefa, como um número inteiro representando MiB, fornecido na solicitação	Numérico

Ações, recursos e chaves de condição para AWS Elastic Disaster Recovery

AWS O Elastic Disaster Recovery (prefixo do serviço:`drs`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Elastic Disaster Recovery
- Tipos de recursos definidos por AWS Elastic Disaster Recovery
- Chaves de condição de AWS Elastic Disaster Recovery

Ações definidas pelo AWS Elastic Disaster Recovery

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o

nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateFailbackClientToRe	Concede permissão para obter o cliente de failback	Gravar	RecoveryInstanceResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
coveryInstanceForDrs [somente permissão]	associado à instância de recuperação				

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateSourceNetworkStack	Concede permissão para associar a CloudFormation pilha à rede de origem	Gravar	SourceNetworkResource*		cloudformation:DescribeStackResource cloudformation:DescribeStacks drs:GetLaunchConfiguration ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DescribeSubnets ec2:DescribeVpcs ec2:ModifyLaunchTemplate
				aws:RequestTag/${TagKey} aws:TagKeys	
BatchCreateVolumeSnapshotGroupForDrs [somente permissão]	Concede permissão para criar lotes de grupo de snapshots de volume	Gravar	RecoveryInstanceResource*		
			SourceServerResource*		
BatchDeleteSnapshotRequestForDrs [somente permissão]	Concede permissão para solicitação de snapshot de exclusão em lote	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateConvertedSnapshotForDrs [somente permissão]	Concede permissão para atualizar um snapshot convertido	Gravar	SourceServerResource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExtendedSourceServer	Concede permissão para estender um servidor de origem	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	drs:DescribeSourceServers drs:GetReplicationConfiguration
CreateLaunchConfigurationTemplate	Concede permissão para criar um modelo de configuração de inicialização	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRecoveryInstanceForDrs [somente permissão]	Concede permissão para criar uma instância de recuperação	Gravar	SourceServerResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateReplicationConfigurationTemplate	Concede permissão para criar modelo de configuração de replicação	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateSecurityGroup ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetEbsDefaultKmsKeyId ec2:GetEbsEncryptionByDefault kms:CreateGrant kms:DescribeKey

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSourceNetwork	Concede permissão para criar uma rede de origem	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeInstances ec2:DescribeVpcs
CreateSourceServerForDrs [somente permissão]	Concede permissão para criar um servidor de fonte	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteJob	Concede permissão para excluir um trabalho	Gravar	JobResource*		
DeleteLaunchAction	Concede permissão para excluir uma ação de lançamento	Gravar	LaunchConfigurationTemplateResource		
			SourceServerResource		
DeleteLaunchConfigurationTemplate	Concede permissão para excluir um modelo de configuração de inicialização	Gravar	LaunchConfigurationTemplateResource*		
DeleteRecoveryInstance	Concede permissão para excluir uma instância de recuperação	Gravar	RecoveryInstanceResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteReplicationConfigurationTemplate	Concede permissão para excluir o modelo de configuração de replicação	Gravar	ReplicationConfigurationTemplateResource*		
DeleteSourceNetwork	Concede permissão para excluir uma rede de origem	Gravar	SourceNetworkResource*		
DeleteSourceServer	Concede permissão para excluir o servidor de origem	Write	SourceServerResource*		
DescribeJobLogItems	Concede permissão para descrever itens de log de tarefas	Read	JobResource*		
DescribeJobs	Concede permissão para descrever tarefas	Leitura			
DescribeLaunchConfigurationTemplates	Concede permissão para descrever um modelo de configuração de inicialização	Leitura			
DescribeRecoveryInstances	Concede permissão para descrever as instâncias de recuperação	Leitura			drs:DescribeSourceServers ec2:DescribeInstances

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeRecoverySnapshots	Concede permissão para descrever os snapshots de recuperação	Leitura	SourceServerResource*		
DescribeReplicationConfigurationTemplates	Concede permissão para descrever o modelo de configuração de replicação	Leitura			
DescribeReplicationServerAssociationsForDrs [somente permissão]	Concede permissão para descrever associações de servidores de replicação	Read			
DescribeSnapshotRequestsForDrs [somente permissão]	Concede permissão para descrever solicitações de snapshot	Leitura			
DescribeSourceNetworks	Concede permissão para descrever redes de origem	Leitura			
DescribeSourceServers	Concede permissão para descrever servidores de origem	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisconnectRecoveryInstance	Concede permissão para desconectar a instância de recuperação	Gravar	RecoveryInstanceResource*		
DisconnectSourceServer	Concede permissão para desconectar o servidor de fonte	Gravar	SourceServerResource*		
ExportSourceNetworkCfnTemplate	Concede permissão para exportar o CloudFormation modelo que contém recursos de rede de origem	Gravar	SourceNetworkResource*		s3:GetBucketLocation s3:GetObject s3:PutObject
				aws:RequestTag/${TagKey} aws:TagKeys	
GetAgentCommandForDrs [somente permissão]	Concede permissão para obter o comando do agente	Read	RecoveryInstanceResource*		
			SourceServerResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAgentConfirmedResumeInfoForDrs [somente permissão]	Concede permissão para obter informações de currículo confirmado pelo agente	Read	RecoveryInstanceResource*		
			SourceServerResource*		
GetAgentInstallationAssetsForDrs [somente permissão]	Concede permissão para obter ativos de instalação do agente	Read			
GetAgentReplicationInfoForDrs [somente permissão]	Concede permissão para obter informações de replicação do agente	Read	RecoveryInstanceResource*		
			SourceServerResource*		
GetAgentRuntimeConfigurationForDrs [somente permissão]	Concede permissão para obter configuração de runtime do agente	Read	RecoveryInstanceResource*		
			SourceServerResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAgentSnapshotCreditsForDrs [somente permissão]	Concede permissão para obter créditos de snapshot do agente	Leitura	RecoveryInstanceResource*		
			SourceServerResource*		
GetChannelCommandsForDrs [somente permissão]	Concede permissão para obter comandos de canal	Leitura			
GetFailbackCommandForDrs [somente permissão]	Concede permissão para obter o comando de failback	Leitura	RecoveryInstanceResource*		
GetFailbackLaunchRequestedForDrs [somente permissão]	Concede permissão para obter o lançamento de failback solicitado	Leitura	RecoveryInstanceResource*		
GetFailbackReplicationConfiguration	Concede permissão para obter a configuração de replicação de failback	Leitura	RecoveryInstanceResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetLaunchConfiguration	Concede permissão para obter a configuração de execução	Read	SourceServerResource*		
GetReplicationConfiguration	Concede permissão para obter a configuração de replicação	Leitura	SourceServerResource*		
GetSuggestedFailbackClientDeviceMappingForDrs [somente permissão]	Concede permissão para obter mapeamento de dispositivos de cliente de failback sugerido	Leitura	RecoveryInstanceResource*		
InitializeService	Concede permissão para inicializar o serviço	Gravar			iam:AddRoleToInstanceProfile iam:CreateInstanceProfile iam:CreateServiceLinkedRole iam:GetInstanceProfile

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
IssueAgentCertificateForDrs [somente permissão]	Concede permissão para emitir um certificado de agente	Gravar	RecoveryInstanceResource*		
			SourceServerResource*		
ListExtensibleSourceServers	Concede permissão para listar servidores de origem extensíveis	Leitura			drs:DescribeSourceServers
ListLaunchActions	Concede permissão para listar ações de lançamento	Leitura	LaunchConfigurationTemplateResource		
			SourceServerResource		
ListStagingAccounts	Concede permissão para listar contas de preparação	Leitura			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura			
NotifyAgentAuthenticationForDrs [somente permissão]	Concede permissão para notificar a autenticação do agente	Write	RecoveryInstanceResource*		
			SourceServerResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
NotifyAgentConnectedForDrs [somente permissão]	Concede permissão para notificar que o agente está conectado	Write	RecoveryInstanceResource*		
			SourceServerResource*		
NotifyAgentDisconnectedForDrs [somente permissão]	Concede permissão para notificar que o agente está desconectado	Write	RecoveryInstanceResource*		
			SourceServerResource*		
NotifyAgentReplicationProgressForDrs [somente permissão]	Concede permissão para notificar o progresso da replicação do agente	Write	RecoveryInstanceResource*		
			SourceServerResource*		
NotifyConsistencyAttainedForDrs [somente permissão]	Concede permissão para notificar consistência atingida	Gravar	RecoveryInstanceResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
NotifyReplicationServerAuthenticationForDrs [somente permissão]	Concede permissão para notificar a autenticação do servidor de replicação	Gravar	RecoveryInstanceResource*		
NotifyVolumeEventForDrs [somente permissão]	Concede permissão para notificar eventos de volume do replicador	Gravar	SourceServerResource*		
PutLaunchAction	Concede permissão para executar uma ação de lançamento	Gravar	LaunchConfigurationTemplateResource		ssm:DescribeDocument
			SourceServerResource		
RetryDataReplication	Concede permissão para repetir a replicação de dados	Gravar	SourceServerResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ReverseReplication	Concede permissão para reverter a replicação	Gravar	RecoveryInstanceResource*		drs:DescribeReplicationConfigurationTemplates drs:DescribeSourceServers ec2:DescribeInstances
				aws:RequestTag/${TagKey} aws:TagKeys	
SendAgentLogsForDrs [somente permissão]	Concede permissão para enviar logs do agente	Write	RecoveryInstanceResource*		
			SourceServerResource*		
SendAgentMetricsForDrs [somente permissão]	Concede permissão para enviar métricas do agente	Write	RecoveryInstanceResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			SourceServerResource*		
SendChannelCommandResultForDrs [somente permissão]	Concede permissão para enviar o resultado do comando do canal	Write			
SendClientLogsForDrs [somente permissão]	Concede permissão para enviar logs de clientes	Write			
SendClientMetricsForDrs [somente permissão]	Concede permissão para enviar métricas de clientes	Write			
SendVolumeStatsForDrs [somente permissão]	Concede permissão para enviar estatísticas de throughput de volume	Gravar	SourceServerResource*		
StartFailbackLaunch	Concede permissão para iniciar a inicialização de failback	Gravar	RecoveryInstanceResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartRecovery	Concede permissão para iniciar a recuperação	Gravar	SourceServerResource*		drs:CreateRecoveryInstanceForDrs drs:ListTagsForResource ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateSnapshot

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:CreateTags ec2:CreateVolume ec2:DeleteLaunchTemplateVersions ec2:DeleteSnapshot ec2:DeleteVolume ec2:DescribeAccountAttributes ec2:DescribeAvailabilityZones ec2:DescribeImages ec2:DescribeInstanceAttribute

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DescribeInstanceStatus ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSnapshots ec2:DescribeSubnets

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DescribeVolumes ec2:DetachVolume ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate ec2:RevokeSecurityGroupEgress ec2:RunInstances ec2:StartInstances ec2:StopInstances ec2:TerminateInstances

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
StartReplication	Concede permissão para iniciar a replicação	Gravar	SourceServerResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartSourceNetworkRecovery	Concede permissão para iniciar a recuperação da rede	Gravar	SourceNetworkResource*		cloudformation:CreateStack cloudformation:DescribeStackResource cloudformation:DescribeStacks cloudformation:UpdateStack drs:GetLaunchConfiguration ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunch

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					Templates ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:ModifyLaunchTemplate s3:GetObject s3:PutObject
				aws:RequestTag/${TagKey} aws:TagKeys	
StartSourceNetworkReplication	Concede permissão para iniciar uma replicação da rede	Gravar	SourceNetworkResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopFailback	Concede permissão para interromper um failback	Gravar	RecoveryInstanceResource*		
StopReplication	Concede permissão para interromper a replicação	Gravar	SourceServerResource*		
StopSourceNetworkReplication	Concede permissão para interromper uma replicação da rede	Gravar	SourceNetworkResource*		
TagResource	Concede permissão para atribuir uma tag de recurso	Tags	JobResource		
			LaunchConfigurationTemplateResource		
			RecoveryInstanceResource		
			ReplicationConfigurationTemplateResource		
			SourceNetworkResource		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			SourceServerResource		
				aws:RequestTag/${TagKey} aws:TagKeys drs:CreateAction	
TerminateRecoveryInstances	Concede permissão para encerrar instâncias de recuperação	Gravar	RecoveryInstanceResource*		drs:DescribeSourceServers ec2:DeleteVolume ec2:DescribeInstances ec2:DescribeVolumes ec2:TerminateInstances

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso	Marcação	JobResource		
			LaunchConfigurationTemplateResource		
			RecoveryInstanceResource		
			ReplicationConfigurationTemplateResource		
			SourceNetworkResource		
			SourceServerResource		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
UpdateAgentBacklogForDrs [somente permissão]	Concede permissão para atualizar o backlog do agente	Write	RecoveryInstanceResource*		
			SourceServerResource*		
UpdateAgentConversionInfoForDrs [somente permissão]	Concede permissão para atualizar informações de conversão do agente	Write	RecoveryInstanceResource*		
			SourceServerResource*		
UpdateAgentReplicationInfoForDrs [somente permissão]	Concede permissão para atualizar informações de replicação do agente	Write	RecoveryInstanceResource*		
			SourceServerResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateAgentReplicationProcessStateForDrs [somente permissão]	Concede permissão para atualizar o estado do processo de replicação do agente	Write	RecoveryInstanceResource*		
			SourceServerResource*		
UpdateAgentSourcePropertiesForDrs [somente permissão]	Concede permissão para atualizar as propriedades de origem do agente	Gravar	RecoveryInstanceResource*		
			SourceServerResource*		
UpdateFailbackClientDeviceMappingForDrs [somente permissão]	Concede permissão para atualizar o mapeamento de dispositivos do cliente de failback	Gravar	RecoveryInstanceResource*		
UpdateFailbackClientLastSeenForDrs [somente permissão]	Concede permissão para atualizar o cliente de failback visto pela última vez	Gravar	RecoveryInstanceResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateFailbackReplicationConfiguration	Concede permissão para atualizar a configuração de replicação de failback	Gravar	RecoveryInstanceResource*		
UpdateLaunchConfiguration	Concede permissão para atualizar uma configuração de execução	Gravar	SourceServerResource*		ec2:DescribeInstances
UpdateLaunchConfigurationTemplate	Concede permissão para atualizar uma configuração de execução	Gravar	LaunchConfigurationTemplateResource*		
UpdateReplicationCertificateForDrs [somente permissão]	Concede permissão para atualizar um certificado de replicação	Gravar	RecoveryInstanceResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateReplicationConfiguration	Concede permissão para atualizar a configuração de replicação	Write	SourceServerResource*		ec2:CreateSecurityGroup ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetEbsDefaultKmsKeyId ec2:GetEbsEncryptionByDefault kms:CreateGrant kms:DescribeKey

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateReplicationConfigurationTemplate	Concede permissão para atualizar o modelo de configuração de replicação	Gravar	ReplicationConfigurationTemplateResource*		ec2:CreateSecurityGroup ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetEbsDefaultKmsKeyId ec2:GetEbsEncryptionByDefault kms:CreateGrant kms:DescribeKey

Tipos de recursos definidos por AWS Elastic Disaster Recovery

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves

são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição de AWS Elastic Disaster Recovery

AWS O Elastic Disaster Recovery define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais

as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString
drs:CreateAction	Filtra o acesso pelo nome de uma ação de API de criação de recurso	String
drs:EC2InstanceARN	Filtra o acesso pela EC2 instância da qual a solicitação foi originada	ARN

Ações, recursos e chaves de condição do Amazon Elastic File System

O Amazon Elastic File System (prefixo do serviço: `elasticfilesystem`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Elastic File System
- Tipos de recursos definidos pelo Amazon Elastic File System
- Chaves de condição do Amazon Elastic File System

Ações definidas pelo Amazon Elastic File System

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de

recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
Backup [somente permissão]	Concede permissão para iniciar um trabalho de backup para um sistema de arquivos existente	Write	file-system*		
ClientMount [somente permissão]	Concede permissão para permitir um acesso de leitura de cliente NFS a um sistema de arquivos	Read	file-system*		
				elasticfilesystem:AccessPointArn elasticfilesystem:AccessedViaMountTarget	
ClientRootAccess [somente permissão]	Concede permissão a um cliente NFS ter acesso root a um sistema de arquivos	Write	file-system*		
				elasticfilesystem:AccessPointArn	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				elasticfilesystem:AccessedViaMountTarget	
ClientWrite [somente permissão]	Concede permissão a um cliente NFS a ter acesso de gravação a um sistema de arquivos	Write	file-system*		
				elasticfilesystem:AccessPointArn elasticfilesystem:AccessedViaMountTarget	
CreateAccessPoint	Concede permissão para criar um ponto de acesso para o sistema de arquivos especificado	Write	file-system*		elasticfilesystem:TagResource
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateFileSystem	Concede permissão para criar um novo sistema de arquivos vazio	Write		aws:RequestTag/${TagKey} aws:TagKeys elasticfilesystem:Encrypted	elasticfilesystem:TagResource
CreateMountTarget	Concede permissão para criar um destino de montagem para um sistema de arquivos	Gravar	file-system*		
CreateReplicationConfiguration	Concede permissão para criar uma nova configuração de replicação	Gravar	file-system*		
CreateTags	Concede permissão para criar ou substituir tags associadas a um sistema de arquivos; obsoleto, consulte TagResource	Tags	file-system*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessPoint	Concede permissão para excluir o ponto de acesso especificado	Write	access-point*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteFileSystem	Concede permissão para excluir um sistema de arquivos, separando permanentemente o acesso ao seu conteúdo	Write	file-system*		
DeleteFileSystemPolicy	Concede permissão para excluir a política de nível de recurso para um sistema de arquivos	Gerenciamento de permissões	file-system*		
DeleteMountTarget	Concede permissão para excluir o destino de monagem especificado	Gravar	file-system*		
DeleteReplicationConfiguration	Concede permissão para excluir a configuração de replicação	Gravar	file-system*		
DeleteTags	Concede permissão para excluir as tags especificadas de um sistema de arquivos; obsoleto, consulte UntagResource	Tags	file-system*		
				aws:TagKeys	
DescribeAccessPoints	Concede permissão para visualizar as descrições dos pontos de acesso do Amazon EFS	List	access-point		
			file-system		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeAccountPreferences	Concede permissão para ver as preferências da conta que estão em vigor	Lista			
DescribeBackupPolicy	Concede permissão para visualizar o BackupPolicy objeto para um sistema de arquivos Amazon EFS	Leitura	file-system*		
DescribeFileSystemPolicy	Concede permissão para visualizar a política de nível de recurso para um sistema de arquivos do Amazon EFS	Leitura	file-system		
DescribeFileSystems	Concede permissão para visualizar a descrição de um sistema de arquivos Amazon EFS especificado pelo sistema de arquivos CreationToken ou FileSystemId; ou para visualizar a descrição de todos os sistemas de arquivos de propriedade do chamador Conta da AWS na AWS região do endpoint que está sendo chamado	Lista	file-system		
DescribeLifecycleConfiguration	Concede permissão para visualizar o LifecycleConfiguration objeto para um sistema de arquivos Amazon EFS	Leitura	file-system*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeMountTargetSecurityGroups	Concede permissão para exibir os grupos de segurança em vigor para um destino de montagem	Read	file-system*		
DescribeMountTargets	Concede permissão para exibir as descrições de todos os destinos de montagem ou um destino de montagem específico para um sistema de arquivos	Leitura	file-system*		
			access-point		
DescribeReplicationConfigurations	Concede permissão para visualizar a descrição de uma configuração de replicação do Amazon EFS especificada por FileSystemId; ou para visualizar a descrição de todas as configurações de replicação de propriedade do chamador Conta da AWS na AWS região do endpoint que está sendo chamado	Lista	file-system		
DescribeTags	Concede permissão para exibir as etiquetas associadas a um sistema de arquivos	Read	file-system*		
ListTagsForResource	Concede permissão para visualizar as etiquetas associadas ao recurso especificado do Amazon EFS	Read	access-point		
			file-system		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ModifyMountTargetSecurityGroups	Concede permissão para modificar o conjunto de grupos de segurança em vigor para um destino de montagem	Write	file-system*		
PutAccountPreferences	Concede permissão para definir as preferências de uma conta	Gravar			
PutBackupPolicy	Concede permissão para ativar ou desativar backups automáticos com o AWS Backup criando um novo BackupPolicy objeto	Gravar	file-system*		
PutFileSystemPolicy	Concede permissão para aplicar uma política de nível de recurso que define as ações permitidas ou negadas de determinados atores para o sistema de arquivos especificado	Gerenciamento de permissões	file-system*		
PutLifecycleConfiguration	Concede permissão para permitir o gerenciamento do ciclo de vida criando um novo objeto LifecycleConfiguration	Gravar	file-system*		
ReplicationRead [somente permissão]	Concede permissão para ler dados do sistema de arquivos para replicação	Leitura	file-system*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ReplicationWrite [somente permissão]	Concede permissão para replicar dados em um sistema de arquivos	Gravar	file-system*		
Restore [somente permissão]	Concede permissão para iniciar um trabalho de restauração para um backup de um sistema de arquivos	Write	file-system*		
TagResource	Concede permissão para criar ou substituir etiquetas associadas ao recurso especificado do Amazon EFS	Marcação	access-point		
			file-system		
				aws:RequestTag/${TagKey} aws:TagKeys elasticfilesystem:CreateAction	
UntagResource	Concede permissão para excluir as etiquetas especificadas de um recurso do Amazon EFS	Marcação	access-point		
			file-system		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
UpdateFileSystem	Concede permissão para atualizar o modo de throughput ou a quantidade de throughput provisionado de um sistema de arquivos existente	Gravar	file-system*		
UpdateFileSystemProtection	Concede permissão para atualizar a proteção do sistema de arquivos de um sistema de arquivos existente	Gravar	file-system*		

Tipos de recursos definidos pelo Amazon Elastic File System

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
file-system	`arn:${Partition}:elasticfilesystem:${Region}:${Account}:file-system/${FileSystemId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
access-point	`arn:${Partition}:elasticfilesystem:${Region}:${Account}:access-point/${AccessPointId}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Elastic File System

O Amazon Elastic File System define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por um par de chave valor da etiqueta que é permitido na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso por um par de chave e valor da etiqueta de um recurso.	Segmento
aws:TagKeys	Filtra o acesso por uma lista de chaves da etiqueta que são permitidas na solicitação	ArrayOfString
elasticfilesystem:AccessPointArn	Filtra o acesso pelo ARN do ponto de acesso usado para montar o sistema de arquivos	ARN
elasticfilesystem:AccessedViaMountTarget	Filtra o acesso se o sistema de arquivos for acessado por meio de destinos de montagem	Bool

Chaves de condição	Descrição	Tipo
elasticfilesystem:CreateAction	Filtra o acesso pelo nome de uma ação de API de criação de recurso	String
elasticfilesystem:Encrypted	Filtra o acesso em que usuários podem criar apenas sistemas de arquivos criptografados ou não criptografados	Bool

Ações, recursos e chaves de condição para o Amazon Elastic Kubernetes Service

O Amazon Elastic Kubernetes Service (prefixo de serviço: `eks`) fornece os seguintes recursos, ações e chaves de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Elastic Kubernetes Service
- Tipos de recursos definidos pelo Amazon Elastic Kubernetes Service
- Chaves de condição para o Amazon Elastic Kubernetes Service

Ações definidas pelo Amazon Elastic Kubernetes Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AccessKubernetesApi [somente permissão]	Concede permissão para visualizar objetos do Kubernetes por meio do console EKS AWS	Leitura	cluster*		
AssociateAccessPolicy	Concede permissão para associar uma política de acesso do Amazon EKS a uma entrada de acesso do Amazon EKS	Gravar	access-entry*		
				eks:policyArn eks:namespaces eks:accessScope	
AssociateEncryptionConfig	Concede permissão para associar a configuração de criptografia a um cluster	Write	cluster*		
AssociateIdentityProviderConfig	Concede permissão para associar uma configuração de provedor de identidade a um cluster	Gravar	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys eks:clientId	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				eks:issuerUrl	
CreateAccessEntry	Concede permissão para criar uma entrada de acesso do Amazon EKS	Gravar	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys eks:principalArn eks:kubernetesGroups eks:username eks:accessEntryType	
CreateAddon	Concede permissão para criar um complemento do Amazon EKS	Write	cluster*		
			podidentityassociation		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateCluster	Concede permissão para criar um cluster do Amazon EKS	Gravar		aws:RequestTag/${TagKey} aws:TagKeys eks:bootstrapClusterCreatorAdminPermissions eks:bootstrapSelfManagedAddons eks:authenticationMode eks:supportType eks:computeConfigEnabled eks:elasticLoadBalancingEnabled	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				eks:blockStorageEnabled	
CreateEksAnywhereSubscription	Concede permissão para criar uma assinatura do EKS Anywhere	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFargateProfile	Concede permissão para criar um perfil do AWS Fargate	Gravar	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNodegroup	Concede permissão para criar um Nodegroup do Amazon EKS	Gravar	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePodIdentityAssociation	Concede permissão para criar uma associação do EKS Pod Identity	Gravar	cluster*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessEntry	Concede permissão para excluir uma entrada de acesso do Amazon EKS	Gravar	access-entry*		
DeleteAddon	Concede permissão para excluir um complemento do Amazon EKS	Write	addon*		
			podidentityassociation		
DeleteCluster	Concede permissão para excluir um cluster do Amazon EKS	Gravar	cluster*		
DeleteEksAnywhereSubscription	Concede permissão para descrever uma assinatura do EKS Anywhere	Gravar	eks-anywhere-subscription*		
DeleteFargateProfile	Concede permissão para excluir um perfil do AWS Fargate	Gravar	fargateprofile*		
DeleteNodegroup	Concede permissão para excluir um Nodegroup do Amazon EKS	Gravar	nodegroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeletePodIdentityAssociation	Concede permissão para excluir uma associação do EKS Pod Identity	Gravar	podidentityassociation*		
DeregisterCluster	Concede permissão para cancelar o registro de um cluster externo	Gravar	cluster*		
DescribeAccessEntry	Concede permissão para descrever uma entrada de acesso do Amazon EKS	Leitura	access-entry*		
DescribeAddon	Concede permissão para recuperar informações descritivas sobre um complemento do Amazon EKS	Leitura	addon*		
DescribeAddonConfiguration	Concede permissão para listar opções de configuração sobre um complemento do Amazon EKS	Leitura			
DescribeAddonVersions	Concede permissão para recuperar informações de versão descritivas sobre os complementos compatíveis com os complementos do Amazon EKS	Read			
DescribeCluster	Concede permissão para recuperar informações descritivas sobre um cluster do Amazon EKS	Leitura	cluster*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeClusterVersions	Concede permissão para recuperar informações descritivas sobre as versões do Kubernetes que os clusters do Amazon EKS suportam	Leitura			
DescribeEksAnywhereSubscription	Concede permissão para descrever uma assinatura do EKS Anywhere	Leitura	eks-anywhere-subscription*		
DescribeFargateProfile	Concede permissão para recuperar informações descritivas sobre um perfil do AWS Fargate associado a um cluster	Leitura	fargateprofile*		
DescribeIdentityProviderConfig	Concede permissão para recuperar informações descritivas sobre uma configuração Idp associada a um cluster	Leitura	identityproviderconfig*		
DescribeInsight	Concede permissão para recuperar informações descritivas de um insight detectado para um cluster especificado	Leitura	cluster*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeNodegroup	Concede permissão para recuperar informações descritivas sobre um nodegroup do Amazon EKS	Leitura	nodegroup*		
DescribePodIdentityAssociation	Concede permissão para descrever uma associação do EKS Pod Identity	Leitura	podidentityassociation*		
DescribeUpdate	Concede permissão para recuperar uma determinada atualização para um determinado Amazon EKS cluster/nodegroup/add -on (na região especificada ou padrão)	Leitura	cluster*		
			addon		
			nodegroup		
DisassociateAccessPolicy	Concede permissão para desassociar uma política de acesso do Amazon EKS de uma entrada de acesso do Amazon EKS	Gravar	access-entry*		
				eks:policyArn eks:namespaces eks:accessScope	
DisassociateIdentityProviderConfig	Concede permissão para excluir uma configuração de Idp associada	Gravar	identityproviderconfig*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAccessEntries	Concede permissão para listar entradas de acesso do Amazon EKS	Lista	cluster*		
ListAccessPolicies	Concede permissão para listar políticas de acesso do Amazon EKS	Lista			
ListAddons	Concede permissão para listar os complementos do Amazon EKS em sua Conta da AWS (na região especificada ou padrão) para um determinado cluster	Lista	cluster*		
ListAssociatedAccessPolicies	Concede permissão para listar políticas de acesso associadas a uma entrada de acesso do Amazon EKS	Lista	access-entry*		
ListClusters	Concede permissão para listar os clusters do Amazon EKS em sua Conta da AWS (na região especificada ou padrão)	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDashboardData	Concede permissão para listar os dados do painel. O painel do Amazon EKS agrega informações sobre recursos de cluster em várias contas e regiões. O painel inclui informações sobre EC2 instâncias e versões do cluster EKS	Leitura	dashboard*		
ListDashboardResources	Concede permissão para listar recursos do painel. O painel do Amazon EKS agrega informações sobre recursos de cluster em várias contas e regiões. O painel inclui informações sobre EC2 instâncias e versões do cluster EKS	Leitura	dashboard*		
ListEksAnywhereSubscriptions	Concede permissão para listar assinaturas do EKS Anywhere	Lista			
ListFargateProfiles	Concede permissão para listar os perfis do AWS Fargate na sua Conta da AWS (na região especificada ou padrão) associados a um determinado cluster	Lista	cluster*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListIdentityProviderConfigs	Concede permissão para listar as configurações do Idp na sua Conta da AWS (na região especificada ou padrão) associada a um determinado cluster	Lista	cluster*		
ListInsights	Concede permissão para listar todos os insights detectados para um cluster especificado	Lista	cluster*		
ListNodegroups	Concede permissão para listar os grupos de nós do Amazon EKS em sua Conta da AWS (na região especificada ou padrão) anexados a um determinado cluster	Lista	cluster*		
ListPodIdentityAssociations	Concede permissão para listar associações do EKS Pod Identity	Lista	cluster*		
ListTagsForResource	Concede permissão para listar etiquetas para o recurso especificado	Leitura	addon		
			cluster		
			dashboard		
			eks-anywhere-subscription		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			fargateprofile		
			identityproviderconfig		
			nodegroup		
ListUpdates	Concede permissão para listar as atualizações de um determinado Amazon EKS cluster/nodegroup/add -on (na região especificada ou padrão)	Lista	cluster*		
			addon		
			nodegroup		
RegisterCluster	Concede permissão para registrar um cluster externo	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Concede permissão para marcar o recurso especificado	Marcação	access-entry		
			addon		
			cluster		
			dashboard		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			eks-anywhere-subscription		
			fargateprofile		
			identityproviderconfig		
			nodegroup		
			podidentityassociation		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar o recurso especificado	Tags	access-entry		
			addon		
			cluster		
			dashboard		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			eks-anywhere-subscription		
			fargateprofile		
			identityproviderconfig		
			nodegroup		
			podidentityassociation		
				aws:TagKeys	
UpdateAccessEntry	Concede permissão para atualizar uma entrada de acesso do Amazon EKS	Gravar	access-entry*		
UpdateAddon	Concede permissão para atualizar configurações de complemento do Amazon EKS, como a versão de VPC-CNI	Write	addon*		
			podidentityassociation		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateClusterConfig	Concede permissão para atualizar as configurações de cluster do Amazon EKS (por exemplo: acesso ao endpoint do servidor de API)	Write	cluster*		
				eks:authenticationMode eks:supportType eks:computeConfigEnabled eks:elasticLoadBalancingEnabled eks:blockStorageEnabled	
UpdateClusterVersion	Concede permissão para atualizar a versão do Kubernetes de um cluster do Amazon EKS	Gravar	cluster*		
UpdateEksAnywhereSubscription	Concede permissão para atualizar uma assinatura do EKS Anywhere	Gravar	eks-anywhere-subscription*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateNodegroupConfig	Concede permissão para atualizar as configurações do grupo de nós do Amazon EKS (por exemplo: min/max/desired capacidade ou rótulos)	Gravar	nodegroup*		
UpdateNodegroupVersion	Concede permissão para atualizar a versão do Kubernetes de um nodegroup do Amazon EKS	Gravar	nodegroup*		
UpdatePodIdentityAssociation	Concede permissão para atualizar uma associação do EKS Pod Identity	Gravar	podidentityassociation*		

Tipos de recursos definidos pelo Amazon Elastic Kubernetes Service

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
cluster	`arn:${Partition}:eks:${Region}:${Account}:cluster/${ClusterName}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
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}

Tipos de recursos	ARN	Chaves de condição
access-entry	`arn:${Partition}:eks:${Region}:${Account}:access-entry/${ClusterName}/${IamIdentityType}/${IamIdentityAccountID}/${IamIdentityName}/${UUID}`	aws:ResourceTag/${TagKey} eks:accessEntryType eks:clusterName eks:kubernetesGroups eks:principalArn eks:username
access-policy	`arn:${Partition}:eks::aws:cluster-access-policy/${AccessPolicyName}`	
dashboard	`arn:${Partition}:eks:${Region}:${Account}:dashboard/${DashboardName}`	aws:ResourceTag/${TagKey}

Chaves de condição para o Amazon Elastic Kubernetes Service

O Amazon Elastic Kubernetes Service define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso por uma chave presente na solicitação que o usuário faz ao serviço EKS	String

Chaves de condição	Descrição	Type
aws:ResourceTag/${TagKey}	Filtra o acesso por uma chave da etiqueta e par de valores	String
aws:TagKeys	Filtra o acesso pela lista de todos os nomes de chave da etiqueta presentes na solicitação que o usuário faz ao serviço EKS	ArrayOfString
eks:accessEntryType	Filtra o acesso pelo tipo de entrada de acesso presente nas solicitações de entrada de acesso que o usuário faz ao serviço EKS	String
eks:accessScope	Filtra o acesso pelo accessScope presente nas solicitações de política de acesso de associação/desassociação que o usuário faz ao serviço EKS	String
eks:authenticationMode	Filtra o acesso pelo authenticationMode presente na solicitação de criação e atualização do cluster	String
eks:blockStorageEnabled	Filtra o acesso pelo parâmetro de armazenamento em bloco ativado na solicitação de criação/atualização do cluster	Bool
eks:bootstrapClusterCreatorAdminPermissions	Filtra o acesso pelo bootstrapClusterCreator AdminPermissions presente na solicitação de criação de cluster	Bool
eks:bootstrapSelfManagedAddons	Filtra o acesso pelos bootstrapSelfManaged complementos presentes na solicitação de criação do cluster	Bool
eks:clientId	Filtra o acesso pelo ClientID presente na solicitação associateIdentityProvider Config que o usuário faz ao serviço EKS	String

Chaves de condição	Descrição	Type
eks:clusterName	Filtra o acesso pelo clusterName presente nas solicitações de entrada de acesso que o usuário faz ao serviço EKS	String
eks:computeConfigEnabled	Filtra o acesso pelo parâmetro compute config enabled na solicitação de criação/atualização do cluster	Bool
eks:elasticLoadBalancingEnabled	Filtra o acesso pelo parâmetro habilitado para balanceamento de carga elástico na solicitação de criação/atualização do cluster	Bool
eks:issuerUrl	Filtra o acesso pelo issuerURL presente na solicitação associateIdentityProvider Config que o usuário faz ao serviço EKS	String
eks:kubernetesGroups	Filtra o acesso pelo kubernetesGroups presente nas solicitações de entrada de acesso que o usuário faz ao serviço EKS	ArrayOfString
eks:namespaces	Filtra o acesso pelos namespaces presentes nas solicitações de política de acesso de associação/desassociação que o usuário faz ao serviço EKS	ArrayOfString
eks:policyArn	Filtra o acesso pela policyArn presente nas solicitações de entrada de acesso que o usuário faz ao serviço EKS	ARN
eks:principalArn	Filtra o acesso pela principalArn presente nas solicitações de entrada de acesso que o usuário faz ao serviço EKS	ARN
eks:supportType	Filtra o acesso pelo supportType presente na solicitação de criação e atualização do cluster	String
eks:username	Filtra o acesso pelo nome de usuário do Kubernetes presente nas solicitações de entrada de acesso que o usuário faz ao serviço EKS	String

Ações, recursos e chaves de condição para o AWS Elastic Load Balancing

AWS O Elastic Load Balancing (prefixo do serviço:`elasticloadbalancing`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Elastic Load Balancing
- Tipos de recursos definidos pelo AWS Elastic Load Balancing
- Chaves de condição para o AWS Elastic Load Balancing

Ações definidas pelo AWS Elastic Load Balancing

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddTags	Concede permissão para adicionar as etiquetas especificadas ao balanceador de carga especificado. Cada load balancer pode ter no máximo 10 etiquetas	Tags	loadbalancer*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:CreateAction	
ApplySecurityGroupsToLoadBalancer	Concede permissão para associar um ou mais grupos de segurança ao balanceador de carga em uma nuvem privada virtual (VPC)	Gravar	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AttachLoadBalancerToSubnets	Concede permissão para adicionar uma ou mais sub-redes ao conjunto de sub-redes configurado para o balanceador de carga especificado	Gravar	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:Subnet	
ConfigureHealthCheck	Concede permissão para especificar as configurações de verificação de integridade a serem usadas ao avaliar o estado de integridade de instâncias de backend	Gravar	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAppCookieStickinessPolicy	Concede permissão para gerar uma ou mais políticas de perdurabilidade com os tempos de vida de sessão persistente que seguem as políticas de um cookie gerado pela aplicação	Gravar	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateLBCookieStickinessPolicy	Concede permissão para gerar uma política de perdurabilidade com tempos de vida de sessão persistente controlados por toda a vida útil do navegador (agente de usuário) ou por um período de expiração especificado	Gravar	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateLoadBalancer	Concede permissão para criar um balanceador de carga	Gravar	loadbalancer		elasticloadbalancing:AddTags

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup elasticloadbalancing:Subnet elasticloadbalancing:Scheme elasticloadbalancing:Listen	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				erProtocol	
CreateLoadBalancerListeners	Concede permissão parpa criar um ou mais listeners para o balanceador de carga especificado	Gravar	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:ListenerProtocol	
CreateLoadBalancerPolicy	Concede permissão para criar uma política com os atributos especificados para o balanceador de carga especificado	Gravar	loadbalancer*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy	
DeleteLoadBalancer	Concede permissão para excluir o balanceador de carga especificado	Gravar	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteLoadBalancerListeners	Concede permissão para excluir os listeners especificados do balanceador de carga especificado	Gravar	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteLoadBalancerPolicy	Concede permissão para excluir a política especificada do balanceador de carga especificado Essa política não deve ser habilitada para nenhum listener	Gravar	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeregisterInstancesFromLoadBalancer	Concede permissão para cancelar o registro das instâncias especificadas do balanceador de carga especificado	Gravar	loadbalancer*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DescribeInstanceHealth	Concede permissão para descrever o estado das instâncias especificadas com relação ao balanceador de carga especificado	Leitura			
DescribeLoadBalancerAttributes	Concede permissão para descrever os atributos do balanceador de carga especificado	Leitura			
DescribeLoadBalancerPolicies	Concede permissão para descrever as políticas especificadas	Leitura			
DescribeLoadBalancerPolicyTypes	Concede permissão para descreve os tipos de políticas do balanceador de carga especificado	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeLoadBalancers	Concede permissão para descrever os balanceadores de carga especificados. Se nenhum load balancer for especificado, a chamada descreverá todos os load balancers	Lista			
DescribeTags	Concede permissão para descrever as etiquetas associadas aos load balancers especificados	Leitura			
DetachLoadBalancerFromSubnets	Concede permissão para remover as sub-redes especificadas do conjunto de sub-redes configuradas para o balanceador de carga	Gravar	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisableAvailabilityZonesForLoadBalancer	Concede permissão para remover as zonas de disponibilidade especificadas do conjunto de zonas de disponibilidade do balanceador de carga especificado	Gravar	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
EnableAvailabilityZonesForLoadBalancer	Concede permissão para adicionar as zonas de disponibilidade especificadas ao conjunto de zonas de disponibilidade do balanceador de carga especificado	Gravar	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyLoadBalancerAttributes	Concede permissão para modificar os atributos do balanceador de carga especificado	Gravar	loadbalancer*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RegisterInstancesWithLoadBalancer	Concede permissão para adicionar as instâncias especificadas ao balanceador de carga especificado	Gravar	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveTags	Concede permissão para remover uma ou mais etiquetas do balanceador de carga especificado	Tags	loadbalancer*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetLoadBalancerListenerSSLCertificate	Concede permissão para definir o certificado que encerra as conexões SSL do listener especificado	Gravar	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SetLoadBalancerPoliciesForBackendServer	Concede permissão para substituir o conjunto de políticas associado à porta especificada na qual o servidor de backend está escutando por um novo conjunto de políticas	Gravar	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetLoadBalancerPoliciesOfListener	Concede permissão para substituir o conjunto atual de políticas para a porta do balanceador de carga especificado pelo conjunto de políticas especificado	Gravar	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy	

Tipos de recursos definidos pelo AWS Elastic Load Balancing

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
loadbalancer	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/${LoadBalancerName}`	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

Chaves de condição para o AWS Elastic Load Balancing

AWS O Elastic Load Balancing define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por um par de chave valor da etiqueta que é permitido na solicitação	Segmento

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso por um par de chave e valor da etiqueta de um recurso.	Segmento
aws:TagKeys	Filtra o acesso por uma lista de chaves da etiqueta que são permitidas na solicitação	ArrayOfString
elasticloadbalancing:CreateAction	Filtra o acesso pelo nome de uma ação de API de criação de recurso	String
elasticloadbalancing:ListenerProtocol	Filtra o acesso pelos protocolos do receptor permitidos na solicitação	ArrayOfString
elasticloadbalancing:ResourceTag/	Filtra o acesso pela string de prefácio de um par de chave e valor de uma etiqueta anexado a um recurso	String
elasticloadbalancing:ResourceTag/${TagKey}	Filtra o acesso pela string de prefácio de um par de chave e valor de uma etiqueta anexado a um recurso	String
elasticloadbalancing:Scheme	Filtra o acesso pelo esquema do balanceador de carga permitido na solicitação	String
elasticloadbalancing:SecurityGroup	Filtra o acesso pelo grupo de segurança IDs permitido na solicitação	ArrayOfString

Chaves de condição	Descrição	Tipo
elasticloadbalancing:SecurityPolicy	Filtra o acesso pelas políticas de segurança SSL permitidas na solicitação	ArrayOfString
elasticloadbalancing:Subnet	Filtra o acesso pela sub-rede IDs que é permitido na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Elastic Load Balancing V2

AWS O Elastic Load Balancing V2 (prefixo do serviço:`elasticloadbalancing`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Elastic Load Balancing V2
- Tipos de recursos definidos pelo AWS Elastic Load Balancing V2
- Chaves de condição do AWS Elastic Load Balancing V2

Ações definidas pelo AWS Elastic Load Balancing V2

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddListenerCertificates	Concede permissão para adicionar os certificados especificados ao listener seguro especificado	Gravar	listener/app*		
			listener/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
AddTags	Concede permissão para adicionar as etiquetas especificadas ao balanceador de carga especificado. Cada load balancer pode ter no máximo 10 etiquetas	Tags	listener-rule/app		
			listener-rule/net		
			listener/app		
			listener/gwy		
			listener/net		
			loadbalancer/app/		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			loadbalancer/gwy/		
			loadbalancer/net/		
			targetgroup		
			truststore		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:CreateAction	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddTrustStoreRevocations	Concede permissão para adicionar revogações a um armazenamento confiável	Gravar	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateListener	Concede permissão para criar um listener para o Application Load Balancer especificado	Gravar	loadbalancer/app/		elasticloadbalancing:AddTags
			loadbalancer/gwy/		
			loadbalancer/net/		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy elasticloadbalancing:ListenerProtocol	
CreateLoadBalancer	Concede permissão para criar um balanceador de carga	Gravar	loadbalancer/app/		elasticloadbalancing:AddTags

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			loadbalancer/gwy/		
			loadbalancer/net/		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup elasticloadbalancing:Subnet elasticloadbalancing:Scheme	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateRule	Concede permissão para criar uma regra para o listener especificado	Gravar	listener/app*		elasticloadbalancing:AddTags
			listener/net*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateTargetGroup	Concede permissão para criar um grupo de destino	Gravar	targetgroup*		elasticloadbalancing:AddTags

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateTrustStore	Concede permissão para criar um armazenamento confiável	Gravar	truststore		elasticloadbalancing:AddTags

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteListener	Concede permissão para excluir o listener especificado	Gravar	listener/app*		
			listener/gwy*		
			listener/net*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteLoadBalancer	Concede permissão para excluir o balanceador de carga especificado	Gravar	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteRule	Concede permissão para excluir a regra especificada	Gravar	listener-rule/app*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			listener-rule/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteSharedTrustStoreAssociation	Concede permissão para excluir a associação de armazenamento confiável compartilhado especificada	Gravar	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteTargetGroup	Concede permissão para excluir o grupo de destino especificado	Gravar	targetgroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteTrustStore	Concede permissão para excluir o armazenamento confiável especificado	Gravar	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeregisterTargets	Concede permissão para cancelar o registro dos destinos especificados no grupo de destino especificado	Gravar	targetgroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DescribeAccountLimits	Concede permissão para descrever os limites de recursos do Elastic Load Balancing para o Conta da AWS	Leitura			
DescribeCapacityReservation	Concede permissão para descrever a reserva de capacidade para um balanceador de carga	Leitura			
DescribeListenerAttributes	Concede permissão para descrever os atributos do receptor especificado	Leitura			
DescribeListenerCertificates	Concede permissão para descrever os certificados do listener seguro especificado	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeListeners	Concede permissão para descrever os listeners especificados ou os listeners do Application Load Balancer especificado	Leitura			
DescribeLoadBalancerAttributes	Concede permissão para descrever os atributos do balanceador de carga especificado	Leitura			
DescribeLoadBalancers	Concede permissão para descrever os balanceadores de carga especificados. Se nenhum load balancer for especificado, a chamada descreverá todos os load balancers	Leitura			
DescribeRules	Concede permissão para descrever as regras especificadas ou as regras do listener especificado	Leitura			
DescribeSSLPolicies	Concede permissão para descrever as políticas especificadas ou todas as políticas usadas para a negociação SSL	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeTags	Concede permissão para descrever as etiquetas associadas ao recurso especificado	Leitura			
DescribeTargetGroupAttributes	Concede permissão para descrever os atributos do grupo de destino especificado	Leitura			
DescribeTargetGroups	Concede permissão para descrever os grupos de destino especificados ou todos os grupos de destino	Leitura			
DescribeTargetHealth	Concede permissão para descrever a integridade dos destinos especificados ou de todos os destinos	Leitura			
DescribeTrustStoreAssociations	Concede permissão para descrever as associações com um armazenamento confiável	Leitura			
DescribeTrustStoreRevocations	Concede permissão para descrever as revogações de armazenamentos confiáveis ou todas as revogações relacionadas a um armazenamento confiável	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeTrustStores	Concede permissão para descrever os armazenamentos confiáveis especificados ou todos os armazenamentos confiáveis	Leitura			
GetResourcePolicy	Concede permissão para recuperar a política de recursos associada ao recurso	Leitura	truststore		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
GetTrustStoreCaCertificatesBundle	Concede permissão para recuperar o pacote de certificados de CA de um armazenamento confiável	Leitura	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetTrustStoreRevocationContent	Concede permissão para recuperar o conteúdo de revogação de um armazenamento confiável	Leitura	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyCapacityReservation	Concede permissão para modificar a reserva de capacidade para um balanceador de carga	Gravar	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ModifyIpPools	Concede permissão para modificar os pools de IP de um balanceador de carga	Gravar	loadbalancer/app/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyListener	Concede permissão para modificar as propriedades especificadas do listener especificado	Gravar	listener/app*		
			listener/gwy*		
			listener/net*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy elasticloadbalancing:ListenerProtocol	
ModifyListenerAttributes	Concede permissão para modificar os atributos do receptor especificado	Gravar	listener/app*		
			listener/gwy*		
			listener/net*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyLoadBalancerAttributes	Concede permissão para modificar os atributos do balanceador de carga especificado	Gravar	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyRule	Concede permissão para modificar a regra especificada	Gravar	listener-rule/app*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			listener-rule/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyTargetGroup	Concede permissão para modificar as verificações de integridade usadas ao avaliar o estado de integridade dos destinos no grupo de destino especificado	Gravar	targetgroup*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyTargetGroupAttributes	Concede permissão para modificar os atributos especificados do grupo de destino especificado	Gravar	targetgroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyTrustStore	Concede permissão para modificar o armazenamento confiável especificado	Gravar	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RegisterTargets	Concede permissão para registrar os destinos especificados no grupo de destino especificado	Gravar	targetgroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveListenerCertificates	Concede permissão para remover os certificados especificados do listener seguro especificado	Gravar	listener/app*		
			listener/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveTags	Concede permissão para remover uma ou mais etiquetas do balanceador de carga especificado	Tags	listener-rule/app		
			listener-rule/net		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			listener/app		
			listener/gwy		
			listener/net		
			loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
			targetgroup		
			truststore		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveTrustStoreRevocations	Concede permissão para remover revogações de um armazenamento confiável	Gravar	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SetIpAddressType	Concede permissão para definir o tipo de endereço IP usado pelas sub-redes do balanceador de carga especificado	Gravar	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetRulePriorities	Concede permissão para definir as prioridades das regras especificadas	Gravar	listener-rule/app*		
			listener-rule/net*		
SetSecurityGroups	Concede permissão para associar os grupos de segurança especificados ao balanceador de carga especificado	Gravar	loadbalancer/app/		
			loadbalancer/net/		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup	
SetSubnets	Concede permissão para habilitar a zona de disponibilidade das sub-redes especificadas para o balanceador de carga especificado	Gravar	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:Subnet	
SetWebAcl [somente permissão]	Concede permissão para dar WebAcl permissão ao WAF	Gravar			

Tipos de recursos definidos pelo AWS Elastic Load Balancing V2

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS Elastic Load Balancing V2

AWS O Elastic Load Balancing V2 define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por um par de chave valor da etiqueta que é permitido na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso por um par de chave e valor da etiqueta de um recurso.	Segmento
aws:TagKeys	Filtra o acesso por uma lista de chaves da etiqueta que são permitidas na solicitação	ArrayOfString
elasticloadbalancing:CreateAction	Filtra o acesso pelo nome de uma ação de API de criação de recurso	String
elasticloadbalancing:ListenerProtocol	Filtra o acesso pelo protocolo de receptor permitido na solicitação	String
elasticloadbalancing:ResourceTag/${TagKey}	Filtra o acesso pela string de prefácio de um par de chave e valor de uma etiqueta anexado a um recurso	String

Chaves de condição	Descrição	Tipo
elasticloadbalancing:Scheme	Filtra o acesso pelo esquema do balanceador de carga permitido na solicitação	String
elasticloadbalancing:SecurityGroup	Filtra o acesso pelo grupo de segurança IDs permitido na solicitação	ArrayOfString
elasticloadbalancing:SecurityPolicy	Filtra o acesso pelas políticas de segurança SSL permitidas na solicitação	ArrayOfString
elasticloadbalancing:Subnet	Filtra o acesso pela sub-rede IDs que é permitido na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o Amazon Elastic MapReduce

O Amazon Elastic MapReduce (prefixo do serviço:`elasticmapreduce`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon Elastic MapReduce
- Tipos de recursos definidos pela Amazon Elastic MapReduce
- Chaves de condição para Amazon Elastic MapReduce

Ações definidas pela Amazon Elastic MapReduce

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

> **Note**
>
> A DescribeJobFlows API está obsoleta e, eventualmente, será removida. Recomendamos que você use ListClusters, DescribeCluster ListSteps, ListInstanceGroups e ListBootstrapActions em vez disso

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AccessAllEventLogs	Concede permissão para visualizar todos os registros de eventos em um servidor de histórico de aplicativos persistente	Gravar	cluster*		
AddInstanceFleet	Concede permissão para adicionar uma frota de instâncias a um cluster em execução	Gravar	cluster*		
AddInstanceGroups	Concede permissão para adicionar grupos de instâncias a um cluster em execução	Gravar	cluster*		
AddJobFlowSteps	Concede permissão para adicionar novas etapas a um cluster em execução	Gravar	cluster*		
				elasticmapreduce:ExecutionRoleArn	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddTags	Concede permissão para adicionar etiquetas a um recurso do Amazon EMR	Tags	cluster		
			editor		
			notebook-execution		
			studio		
				aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
AttachEditor [somente permissão]	Concede permissão para anexar cadernos do EMR a um mecanismo de computação	Gravar	editor*		
CancelSteps	Concede permissão para cancelar uma ou mais etapas pendentes em um cluster em execução	Gravar	cluster*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateEditor [somente permissão]	Concede permissão para criar um caderno do EMR	Gravar	cluster		
				aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
CreatePersistentAppUI	Concede permissão para criar um servidor de histórico de aplicações persistente	Gravar	cluster*		
CreateRepository [somente permissão]	Concede permissão para criar um repositório de cadernos do EMR	Gravar			
CreateSecurityConfiguration	Concede permissão para criar uma configuração de segurança	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateStudio	Concede permissão para criar um EMR Studio	Gravar		aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
CreateStudioPresignedUrl	Concede permissão para iniciar um EMR Studio usando o modo de autenticação do IAM	Gravar	studio*		
CreateStudioSessionMapping	Concede permissão para criar um mapeamento de sessões do EMR Studio	Gravar	studio*		
DeleteEditor [somente permissão]	Concede permissão para excluir um caderno do EMR	Gravar	editor*		
DeleteRepository [somente permissão]	Concede permissão para excluir um repositório de cadernos do EMR	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteSecurityConfiguration	Concede permissão para excluir uma configuração de segurança	Gravar			
DeleteStudio	Concede permissão para excluir um EMR Studio	Gravar	studio*		
DeleteStudioSessionMapping	Concede permissão para excluir um mapeamento de sessões do EMR Studio	Gravar	studio*		
DeleteWorkspaceAccess [somente permissão]	Concede permissão para evitar que uma identidade abra um espaço de trabalho colaborativo	Gerenciamento de permissões	editor*		
DescribeCluster	Concede permissão para obter detalhes sobre um cluster, incluindo status, configuração de hardware e software, configurações da VPC e etc	Leitura	cluster*		
DescribeEditor [somente permissão]	Concede permissão para visualizar informações sobre um caderno, incluindo status, usuário, função, etiquetas, local e muito mais	Leitura	editor*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeJobFlows	Concede permissão para descrever detalhes de clusters (fluxos de trabalhos). Esta API está defasada e eventualmente será removida. Recomendamos que você use ListClusters, DescribeCluster ListSteps, ListInstanceGroups e ListBootstrapActions em vez disso	Leitura	cluster*		
DescribeNotebookExecution	Concede permissão para visualizar informações sobre a execução de um caderno	Leitura	notebook-execution*		
DescribePersistentAppUI	Concede permissão para descrever um servidor de histórico de aplicações persistente	Leitura	cluster*		
DescribeReleaseLabel	Concede permissão para visualizar informações sobre uma versão do EMR, como quais aplicações são compatíveis	Leitura			
DescribeRepository [somente permissão]	Concede permissão para descrever um repositório de cadernos do EMR	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeSecurityConfiguration	Concede permissão para obter detalhes de uma configuração de segurança	Leitura			
DescribeStep	Concede permissão para obter detalhes sobre uma etapa do cluster	Leitura	cluster*		
DescribeStudio	Concede permissão para visualizar informações sobre um EMR Studio	Leitura	studio*		
DetachEditor [somente permissão]	Concede permissão para desvincular um caderno do EMR a um mecanismo de computação	Gravar	editor*		
GetAutoTerminationPolicy	Concede permissão para recuperar a política de encerramento automático associada a um cluster	Leitura	cluster*		
GetBlockPublicAccessConfiguration	Concede permissão para recuperar a configuração de acesso público do bloco EMR para Conta da AWS o na região	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetClusterSessionCredentials	Concede permissão para recuperar credenciais básicas HTTP associadas a um determinado perfil de execução do IAM para um cluster do EMR habilitado para controle de acesso refinado	Gravar	cluster*		
				elasticmapreduce:ExecutionRoleArn	
GetManagedScalingPolicy	Concede permissão para recuperar a política de escalabilidade gerenciada associada a um cluster	Leitura	cluster*		
GetOnClusterAppUIPresignedURL	Concede permissão para obter um URL pré-assinado para um servidor de histórico de aplicações em execução no cluster	Gravar	cluster*		
GetPersistentAppUIPresignedURL	Concede permissão para criar um URL pré-assinado para um servidor de histórico de aplicações persistente	Gravar	cluster*		
				elasticmapreduce:ExecutionRoleArn	
GetStudioSessionMapping	Concede permissão para visualizar informações sobre um mapeamento de sessões do EMR Studio	Leitura	studio*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
LinkRepository [somente permissão]	Concede permissão para vincular um repositório de cadernos do EMR a cadernos do EMR	Gravar			
ListBootstrapActions	Concede permissão para obter detalhes sobre as ações de bootstrap associadas a um cluster	Leitura	cluster*		
ListClusters	Concede permissão para obter o status dos clusters acessíveis	Lista			
ListEditors [somente permissão]	Concede permissão para listar as informações de resumo dos cadernos do EMR acessíveis	Lista			
ListInstanceFleets	Concede permissão para obter detalhes de frotas de instâncias em um cluster	Leitura	cluster*		
ListInstanceGroups	Concede permissão para obter detalhes de grupos de instâncias em um cluster	Leitura	cluster*		
ListInstances	Concede permissão para obter detalhes sobre as EC2 instâncias da Amazon em um cluster	Leitura	cluster*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListNotebookExecutions	Concede permissão para listar informações resumidas de execuções de cadernos	Lista			
ListReleaseLabels	Concede permissão para listar e filtrar as versões do EMR disponíveis na região atual	Lista			
ListRepositories [somente permissão]	Concede permissão para listar repositórios existentes de cadernos do EMR	Lista			
ListSecurityConfigurations	Concede permissão para listar as configurações de segurança disponíveis nessa conta pelo nome, junto com datas e horas de criação	Lista			
ListSteps	Concede permissão para listar as etapas associadas a um cluster	Leitura	cluster*		
ListStudioSessionMappings	Concede permissão para listar informações resumidas sobre mapeamentos de sessões do EMR Studio	Lista			
ListStudios	Concede permissão para listar informações resumidas sobre o EMR Studio	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListSupportedInstanceTypes	Concede permissão para listar os tipos de EC2 instância da Amazon que uma versão do Amazon EMR suporta	Lista			
ListWorkspaceAccessIdentities [somente permissão]	Concede permissão para listar identidades que obtêm acesso a um espaço de trabalho	Lista	editor*		
ModifyCluster	Concede permissão para alterar as configurações do cluster, como o número de etapas que podem ser executadas simultaneamente para um cluster	Gravar	cluster*		
ModifyInstanceFleet	Concede permissão para alterar as capacidades Sob demanda de destino e Spot de destino para uma frota de instâncias	Gravar	cluster*		
ModifyInstanceGroups	Concede permissão para alterar o número e a configuração das EC2 instâncias de um grupo de instâncias	Gravar	cluster		
OpenEditorInConsole [somente permissão]	Concede permissão para iniciar o editor de cadernos do Jupyter para cadernos do EMR a partir do console	Gravar	editor* cluster		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutAutoScalingPolicy	Concede permissão para criar ou atualizar uma política de escalabilidade automática para um grupo de instâncias principal ou grupo de instâncias de tarefas	Gravar	cluster*		
PutAutoTerminationPolicy	Concede permissão para criar ou atualizar a política de encerramento automático associada a um cluster	Gravar	cluster*		
PutBlockPublicAccessConfiguration	Concede permissão para criar ou atualizar a configuração de acesso público do bloco EMR para o Conta da AWS na região	Gerenciamento de permissões			
PutManagedScalingPolicy	Concede permissão para criar ou atualizar a política de escalabilidade gerenciada associada a um cluster	Gravar	cluster*		
PutWorkspaceAccess [somente permissão]	Concede permissão para permitir que uma identidade abra um espaço de trabalho colaborativo	Gerenciamento de permissões	editor*		
RemoveAutoScalingPolicy	Concede permissão para remover uma política de escalabilidade automática de um grupo de instâncias	Gravar	cluster*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RemoveAutoTerminationPolicy	Concede permissão para remover a política de encerramento automático associada a um cluster	Gravar	cluster*		
RemoveManagedScalingPolicy	Concede permissão para remover a política de escalabilidade gerenciada associada a um cluster	Gravar	cluster*		
RemoveTags	Concede permissão para remover etiquetas de um recurso do Amazon EMR	Tags	cluster		
			editor		
			notebook-execution		
			studio		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RunJobFlow	Concede permissão para criar e iniciar um cluster (fluxo de trabalho)	Gravar		aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	iam:PassRole
SetKeepJobFlowAliveWhenNoSteps	Concede permissão para adicionar e remover o encerramento automático após a execução da etapa de um cluster	Gravar	cluster*		
SetTerminationProtection	Concede permissão para adicionar e remover a proteção contra encerramento para um cluster	Gravar	cluster*		
SetUnhealthyNodeReplacement	Concede permissão para habilitar ou desabilitar a substituição de nó não íntegro de um cluster	Gravar	cluster*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SetVisibleToAllUsers	Concede permissão para definir se todos os usuários do AWS Identity and Access Management (IAM) Conta da AWS no podem visualizar um cluster. Esta API está defasada e seu cluster pode estar visível para todos os usuários de sua conta. Para restringir o acesso ao cluster usando uma política do IAM, consulte AWS Identity and Access Management for Amazon EMR (https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-plan-access-iam .html)	Gravar	cluster*		
StartEditor [somente permissão]	Concede permissão para iniciar um caderno do EMR	Gravar	editor*		
			cluster		
StartNotebookExecution	Concede permissão para iniciar a execução de um caderno do EMR	Gravar	cluster*		
			editor*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
StopEditor [somente permissão]	Concede permissão para desligar um caderno do EMR	Gravar	editor*		
StopNotebookExecution	Concede permissão para interromper a execução de um caderno	Gravar	notebook-execution*		
TerminateJobFlows	Concede permissão para terminar um cluster (fluxo de trabalho)	Gravar	cluster*		
UnlinkRepository [somente permissão]	Concede permissão para desvincular um repositório dos cadernos do EMR dos cadernos do EMR	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateEditor [somente permissão]	Concede permissão para atualizar um caderno do EMR	Gravar	editor*		
UpdateRepository [somente permissão]	Concede permissão para atualizar um repositório de caderno do EMR	Gravar			
UpdateStudio	Concede permissão para atualizar informações sobre um EMR Studio	Gravar	studio*		
UpdateStudioSessionMapping	Concede permissão para atualizar um mapeamento de sessões do EMR Studio	Gravar	studio*		
ViewEventsFromAllClustersInConsole [somente permissão]	Concede permissão para usar o console do EMR para exibir eventos de todos os clusters	Lista			

Tipos de recursos definidos pela Amazon Elastic MapReduce

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição para Amazon Elastic MapReduce

O Amazon Elastic MapReduce define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso se o par de etiqueta e valor é fornecido com a ação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por par de etiqueta e valor associado a um recurso do Amazon EMR	String
aws:TagKeys	Filtra o acesso se as chaves de etiqueta são fornecidas com a ação, independentemente do valor da etiqueta	ArrayOfString
elasticmapreduce:ExecutionRoleArn	Filtra o acesso com base em se o ARN da função de execução é fornecido com a ação	ARN
elasticmapreduce:RequestTag/${TagKey}	Filtra o acesso se o par de etiqueta e valor é fornecido com a ação	String
elasticmapreduce:ResourceTag/${TagKey}	Filtra o acesso por par de etiqueta e valor associado a um recurso do Amazon EMR	String

Ações, recursos e chaves de condição do Amazon Elastic Transcoder

O Amazon Elastic Transcoder (prefixo de serviço: `elastictranscoder`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Elastic Transcoder
- Tipos de recursos definidos pelo Amazon Elastic Transcoder
- Chaves de condição do Amazon Elastic Transcoder

Ações definidas pelo Amazon Elastic Transcoder

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de

condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelJob	Cancelar um trabalho que o Elastic Transcoder não começou a processar	Gravar	job*		
CreateJob	Criar um trabalho	Gravar	pipeline*		
			preset*		
CreatePipeline	Crie um pipeline	Gravar			
CreatePreset	Criar uma predefinição	Gravar			
DeletePipeline	Apagar um pipeline	Write	pipeline*		
DeletePreset	Excluir uma predefinição	Write	preset*		
ListJobsByPipeline	Obter uma lista dos trabalhos atribuídos a um pipeline	Lista	pipeline*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListJobsByStatus	Obtenha informações sobre todos os trabalhos associados ao atual Conta da AWS que têm um status especificado	Lista			
ListPipelines	Obtenha uma lista dos pipelines associados ao atual Conta da AWS	Lista			
ListPresets	Obtenha uma lista de todas as predefinições associadas à atual Conta da AWS	Lista			
ReadJob	Obter informações detalhadas sobre um trabalho	Read	job*		
ReadPipeline	Obter informações detalhadas sobre um pipeline	Leitura	pipeline*		
ReadPreset	Obter informações detalhadas sobre uma predefinição	Leitura	preset*		
TestRole	Testar as configurações de um pipeline para garantir que o Elastic Transcoder possa criar e processar trabalhos	Write			
UpdatePipeline	Atualizar as configurações de um pipeline	Write	pipeline*		
UpdatePipelineNotifications	Atualizar apenas as notificações do Amazon Simple Notification Service (Amazon SNS) para um pipeline	Gravar	pipeline*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdatePipelineStatus	Pausar ou reativar um pipeline de modo que o pipeline interrompa ou reinicie o processamento de trabalhos, atualize o status do pipeline	Gravar	pipeline*		

Tipos de recursos definidos pelo Amazon Elastic Transcoder

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
job	`arn:${Partition}:elastictranscoder:${Region}:${Account}:job/${JobId}`	
pipeline	`arn:${Partition}:elastictranscoder:${Region}:${Account}:pipeline/${PipelineId}`	
preset	`arn:${Partition}:elastictranscoder:${Region}:${Account}:preset/${PresetId}`	

Chaves de condição do Amazon Elastic Transcoder

O Elastic Transcoder não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o Amazon Elastic VMware Service

O Amazon Elastic VMware Service (prefixo do serviço:`evs`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Elastic VMware Service
- Tipos de recursos definidos pelo Amazon Elastic VMware Service
- Chaves de condição para o Amazon Elastic VMware Service

Ações definidas pelo Amazon Elastic VMware Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateEnvironment	Concede permissão para criar um ambiente Amazon EVS	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateEnvironmentHost	Concede permissão para adicionar um host a um ambiente Amazon EVS	Gravar	environment*		
DeleteEnvironment	Concede permissão para excluir um ambiente Amazon EVS	Gravar	environment*		
DeleteEnvironmentHost	Concede permissão para excluir um host de um ambiente Amazon EVS	Gravar	environment*		
GetEnvironment	Concede permissão para obter um ambiente Amazon EVS	Leitura	environment*		
ListEnvironmentHosts	Concede permissão para recuperar uma lista de hosts associados a um ambiente Amazon EVS	Lista	environment*		
ListEnvironmentVlans	Concede permissão para recuperar uma lista do ambiente Amazon EVS VLANs	Lista	environment*		
ListEnvironments	Concede permissão para recuperar uma lista de ambientes Amazon EVS em uma conta	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar as etiquetas em um ARN de recurso especificado	Leitura	environment		
TagResource	Concede permissão para marcar um ARN de recurso especificado	Tags	environment*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover etiquetas de UM ARN de recurso especificado	Tags	environment*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Tipos de recursos definidos pelo Amazon Elastic VMware Service

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso

também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
environment	`arn:${Partition}:evs:${Region}:${Account}:environment/${EnvironmentIdentifier}`	aws:ResourceTag/${TagKey}

Chaves de condição para o Amazon Elastic VMware Service

O Amazon Elastic VMware Service define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por um par de chave valor da etiqueta que é permitido na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso por um par de chave e valor da etiqueta de um recurso.	Segmento
aws:TagKeys	Filtra o acesso por uma lista de chaves da etiqueta que são permitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para a Amazon ElastiCache

A Amazon ElastiCache (prefixo do serviço:`elasticache`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon ElastiCache
- Tipos de recursos definidos pela Amazon ElastiCache
- Chaves de condição para a Amazon ElastiCache

Ações definidas pela Amazon ElastiCache

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

> **Note**
>
> Ao criar uma ElastiCache política no IAM, você deve usar o caractere curinga "*" para o bloco de recursos. Para obter informações sobre o uso das seguintes ações de ElastiCache API em uma política do IAM, consulte ElastiCache Ações e IAM no Guia ElastiCache do usuário da Amazon.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddTagsToResource	Concede permissão para adicionar tags a um ElastiCache recurso	Tags	cluster		
			parameter group		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			replicationgroup		
			reserved-instance		
			securitygroup		
			serverlesscache		
			serverlesscachesnapshot		
			snapshot		
			subnetgroup		
			user		
			usergroup		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
AuthorizeCacheSecurityGroupIngress	Concede permissão para autorizar um grupo EC2 de segurança em um grupo ElastiCache de segurança	Gravar	securitygroup*		ec2:AuthorizeSecurityGroupIngress
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchApplyUpdateAction	Concede permissão para aplicar atualizações ElastiCache de serviço a conjuntos de clusters e grupos de replicação	Gravar	cluster		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs s3:GetObject
			replicationgroup		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchStopUpdateAction	Concede permissão para impedir que atualizações de ElastiCache serviço sejam executadas em um conjunto de clusters	Gravar	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
CompleteMigration	Concede permissão para concluir uma migração on-line de dados do Redis hospedado na Amazon EC2 para ElastiCache	Gravar	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
Connect	Concede permissão para se conectar como um ElastiCache usuário especificado a um grupo de ElastiCache replicação ou cache sem ElastiCache servidor	Gravar	user*		
			replicationgroup		
			serverlesscache		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CopyServerlessCacheSnapshot	Concede permissão para fazer uma cópia de um snapshot existente de cache com tecnologia sem servidor	Gravar	serverlesscachesnapshot*	aws:ResourceTag/${TagKey} elasticache:KmsKeyId	elasticache:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CopySnapshot	Concede permissão para fazer uma cópia de um snapshot existente	Write	snapshot*		elasticache:AddTagsToResource s3:DeleteObject s3:GetBucketAcl s3:PutObject

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys elasticache:KmsKeyId	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateCacheCluster	Concede permissão para criar um cluster de cache	Write	parameter group*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs elasticache:AddTagsToResource s3:GetObject

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			cluster	aws:RequestTag/${TagKey} aws:TagKeys elasticache:CacheNodeType elasticache:EngineVersion elasticache:EngineType elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				elasticache:CacheParameterGroupName	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			replicationgroup	elasticache:CacheNodeType elasticache:EngineVersion elasticache:EngineType elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:CacheParameterGroupName	
			securitygroup		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			snapshot		
			subnetgroup		
				aws:ResourceTag/${TagKey}	
CreateCacheParameterGroup	Concede permissão para criar um grupo de parâmetros	Write	parametergroup*		elasticache:AddTagsToResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys elasticache:CacheParameterGroupName	
CreateCacheSecurityGroup	Concede permissão para criar um grupo de segurança de cache	Write	securitygroup*		elasticache:AddTagsToResource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateCacheSubnetGroup	Concede permissão para criar um grupo de sub-redes de cache	Write	subnetgroup*		elasticache:AddTagsToResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateGlobalReplicationGroup	Concede permissão para criar um grupo de replicação global	Write	globalreplicationgroup*		
			replicationgroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
CreateReplicationGroup	Concede permissão para criar um grupo de replicação	Gravar	parametergroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs elasticache:AddTagsToResource s3:GetObject
			cluster		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			globalreplicationgroup	elasticache:NumNodeGroups elasticache:CacheNodeType elasticache:ReplicasPerNodeGroup elasticache:EngineVersion elasticache:EngineType elasticache:AtRestEncryptionEnabled elasticache:TransitEncryptionEnabled elasticache:AutomaticFailov	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				erEnabled elasticache:MultiAZEnabled elasticache:ClusterModeEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:KmsKeyId elasticache:CacheParameterGroupName	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			replicationgroup	aws:RequestTag/${TagKey} aws:TagKeys elasticache:NumNodeGroups elasticache:CacheNodeType elasticache:ReplicasPerNodeGroup elasticache:EngineVersion elasticache:EngineType elasticache:AtRestEncryptionEnabled	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				elasticache:TransitEncryptionEnabled elasticache:AutomaticFailoverEnabled elasticache:MultiAZEnabled elasticache:ClusterModeEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:KmsKeyId	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				elasticache:CacheParameterGroupName	
			securitygroup		
			snapshot		
			subnetgroup		
			usergroup		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateServerlessCache	Concede permissão para criar um cache com tecnologia sem servidor	Gravar	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

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				elasticache:MinimumECPUPerSecond elasticache:MaximumECPUPerSecond	s3:GetObject
			serverlessscachesnapshot	aws:ResourceTag/${TagKey}	
			snapshot	aws:ResourceTag/${TagKey}	
			usergroup	aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateServerlessCacheSnapshot	Concede permissão para criar uma cópia de um cache com tecnologia sem servidor em um momento específico	Gravar	serverlesscache*	aws:ResourceTag/${TagKey}	elasticache:AddTagsToResource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			serverlesscachesnapshot*	aws:ResourceTag/${TagKey} elasticache:KmsKeyId	
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshot	Concede permissão para criar uma cópia de um cluster Redis inteiro em um momento específico	Gravar	snapshot*	aws:RequestTag/${TagKey} aws:TagKeys elasticache:KmsKeyId	elasticache:AddTagsToResource s3:DeleteObject s3:GetBucketAcl s3:PutObject
			cluster		
			replicationgroup		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
CreateUser	Concede permissão para criar um usuário do Redis. Há suporte para usuários do Redis 6.0 em diante.	Gravar	user*		elasticache:AddTagsToResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys elasticache:UserAuthenticationMode	
CreateUserGroup	Concede permissão para criar um grupo de usuários do Redis. Há suporte para grupos do Redis 6.0 em diante.	Gravar	user*		elasticache:AddTagsToResource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			usergroup*	aws:RequestTag/${TagKey} aws:TagKeys	
				aws:ResourceTag/${TagKey}	
DecreaseNodeGroupsInGlobalReplicationGroup	Concede permissão para diminuir o número de grupos de nós em grupos de replicação globais	Write	globalreplicationgroup*		
				elasticache:NumNodeGroups	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DecreaseReplicaCount	Concede permissão para diminuir o número de réplicas em um grupo de replicação Redis (modo de cluster desabilitado) ou o número de nós de réplica em um ou mais grupos de nós (fragmentos) de um grupo de replicação Redis (modo de cluster habilitado)	Write	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey} elasticache:ReplicasPerNodeGroup	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteCacheCluster	Concede permissão para excluir um cluster provisionado anteriormente	Write	cluster*	aws:ResourceTag/${TagKey}	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			snapshot		
DeleteCacheParameterGroup	Concede permissão para excluir o grupo de parâmetros de cache especificado	Write	parametergroup*		
				aws:ResourceTag/${TagKey} elasticache:CacheParameterGroupName	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteCacheSecurityGroup	Concede permissão para excluir um grupo de segurança de cache	Write	securitygroup*		
				aws:ResourceTag/${TagKey}	
DeleteCacheSubnetGroup	Concede permissão para excluir um grupo de sub-redes de cache	Write	subnetgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	
DeleteGlobalReplicationGroup	Concede permissão para excluir um grupo de replicação global existente	Write	globalreplicationgroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteReplicationGroup	Concede permissão para excluir um grupo de replicação existente	Gravar	replicationgroup*	aws:ResourceTag/${TagKey}	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			snapshot		
DeleteServerlessCache	Concede permissão para excluir um cache com tecnologia sem servidor	Gravar	serverlesscache*	aws:ResourceTag/${TagKey}	ec2:DescribeTags
			serverlesscachesnapshot		
DeleteServerlessCacheSnapshot	Concede permissão para excluir um snapshot de cache com tecnologia sem servidor	Gravar	serverlesscachesnapshot*	aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteSnapshot	Concede permissão para excluir um snapshot existente	Write	snapshot*		
				aws:ResourceTag/${TagKey}	
DeleteUser	Concede permissão para excluir um usuário existente e, portanto, removê-lo de todos os grupos de usuários e grupos de replicação aos quais ele foi atribuído	Write	user*		
				aws:ResourceTag/${TagKey}	
DeleteUserGroup	Concede permissão para excluir um grupo de usuários existente	Write	usergroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheClusters	Concede permissão para listar informações sobre clusters de cache provisionados	Lista	cluster*		
				aws:ResourceTag/${TagKey}	
DescribeCacheEngineVersions	Concede permissão para listar mecanismos de cache disponíveis e suas versões	Lista			
DescribeCacheParameterGroups	Concede permissão para listar descrições de grupos de parâmetros de cache	List	parametergroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
DescribeCacheParameters	Concede permissão para recuperar a lista de parâmetros detalhada de um grupo de parâmetros de cache específico	List	parametergroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheSecurityGroups	Concede permissão para listar descrições do grupo de segurança de cache	List	securitygroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheSubnetGroups	Concede permissão para listar descrições de grupos de sub-redes de cache	List	subnetgroup*		
				aws:ResourceTag/${TagKey}	
DescribeEngineDefaultParameters	Concede permissão para retornar as informações sobre o mecanismo padrão e parâmetros do sistema do mecanismo de cache especificado	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeEvents	Concede permissão para listar eventos relacionados a clusters, grupos de segurança de cache e grupos de parâmetros de cache	List			
DescribeGlobalReplicationGroups	Concede permissão para listar informações sobre grupos de replicação globais	List	globalreplicationgroup*		
DescribeReplicationGroups	Concede permissão para listar informações sobre grupos de replicação provisionados	List	replicationgroup*		
				aws:ResourceTag/${TagKey}	
DescribeReservedCacheNodes	Concede permissão para listar informações sobre nós de cache reservados comprados	List	reserved-instance*		
				aws:ResourceTag/${TagKey}	
DescribeReservedCacheNodesOfferings	Concede permissão para listar ofertas disponíveis de nós de cache reservados	Lista			
DescribeServerlessCacheSnapshots	Concede permissão para listar informações sobre snapshots de caches com tecnologia sem servidor	Lista	serverlesscachesnapshot*	aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			serverlesscache	aws:ResourceTag/${TagKey}	
DescribeServerlessCaches	Concede permissão para listar caches com tecnologia sem servidor	Lista	serverlesscache*	aws:ResourceTag/${TagKey}	
DescribeServiceUpdates	Concede permissão para listar detalhes das atualizações do serviço	List			
DescribeSnapshots	Concede permissão para listar informações sobre snapshots de grupos de replicação ou clusters	List	snapshot*		
				aws:ResourceTag/${TagKey}	
DescribeUpdateActions	Concede permissão para listar detalhes das ações de atualização de um conjunto de clusters ou grupos de replicação	List	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
DescribeUserGroups	Concede permissão para listar informações sobre grupos de usuários do Redis	List	usergroup*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeUsers	Concede permissão para listar informações sobre usuários do Redis	List	user*		
				aws:ResourceTag/${TagKey}	
DisassociateGlobalReplicationGroup	Concede permissão para remover um grupo de replicação secundário do grupo de replicação global	Gravar	globalreplicationgroup*		
ExportServerlessCacheSnapshot	Concede permissão para exportar uma cópia de um cache com tecnologia sem servidor em um momento específico a um bucket do s3	Gravar	serverlesscachesnapshot*	aws:ResourceTag/${TagKey}	s3:DeleteObject s3:ListAllMyBuckets s3:PutObject
FailoverGlobalReplicationGroup	Concede permissão para fazer failover da região primária para uma região secundária selecionada de um grupo de replicação global	Write	globalreplicationgroup*		
IncreaseNodeGroupsInGlobalReplicationGroup	Concede permissão para aumentar o número de grupos de nós em um grupo de replicação global	Write	globalreplicationgroup*		
				elasticache:NumNodeGroups	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
IncreaseReplicaCount	Concede permissão para aumentar o número de réplicas em um grupo de replicação Redis (modo de cluster desabilitado) ou o número de nós de réplica em um ou mais grupos de nós (fragmentos) de um grupo de replicação Redis (modo de cluster habilitado)	Gravar	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey} elasticache:ReplicasPerNodeGroup	
InterruptClusterAzPower [somente permissão]	Concede permissão para testar uma interrupção de energia AZ para um recurso ElastiCache	Gravar	replicationgroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
ListAllowedNodeTypeModifications	Concede permissão para listar o tipo de nó disponível que pode ser usado para dimensionar um cluster ou grupo de replicação Redis específico	Lista	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
ListTagsForResource	Concede permissão para listar tags para um ElastiCache recurso	Leitura	cluster		
			parametergroup		
			replicationgroup		
			reserved-instance		
			securitygroup		
			serverlesscache		
			serverlesscachesnapshot		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			snapshot		
			subnetgroup		
			user		
			usergroup		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ModifyCacheCluster	Concede permissão para modificar configurações de um cluster	Write	cluster*	elasticache:CacheNodeType elasticache:EngineVersion elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:CacheParameterGroupName	
			parameter group		
			securitygroup		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
ModifyCacheParameterGroup	Concede permissão para modificar os parâmetros de um grupo de parâmetros de cache	Write	parametergroup*		
				aws:ResourceTag/${TagKey} elasticache:CacheParameterGroupName	
ModifyCacheSubnetGroup	Concede permissão para modificar um grupo de sub-redes de cache existente	Write	subnetgroup*		
				aws:ResourceTag/${TagKey}	
ModifyGlobalReplicationGroup	Concede permissão para modificar configurações de um grupo de replicação global	Write	globalreplicationgroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				elasticache:CacheNodeType elasticache:EngineVersion elasticache:AutomaticFailoverEnabled	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ModifyReplicationGroup	Concede permissão para modificar as configurações de um grupo de replicação	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

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				tEncryptionEnabled elasticache:ClusterModeEnabled	
			parametergroup		
			securitygroup		
			usergroup		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ModifyReplicationGroupShardConfiguration	Concede permissão para adicionar fragmentos, remover fragmentos ou reequilibrar os keyspaces entre fragmentos existentes de um grupo de replicação	Gravar	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey} elasticache:NumNodeGroups	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ModifyServerlessCache	Concede permissão para modificar os parâmetros para um cache com tecnologia sem servidor	Gravar	serverlesscache*	aws:ResourceTag/${TagKey} elasticache:EngineVersion elasticache:SnapshotRetentionLimit elasticache:MinimumDataStorage elasticache:MaximumDataStorage elasticache:DataStorageUnit elasticache:MinimumECPUPerSecond elasticache:Maximu	ec2:DescribeSecurityGroups ec2:DescribeTags

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				mECPUPerSecond	
			usergroup	aws:ResourceTag/${TagKey}	
ModifyUser	Concede permissão para alterar a string de and/or acesso da (s) senha (s) de usuário do Redis	Gravar	user*		
				aws:ResourceTag/${TagKey} elasticache:UserAuthenticationMode	
ModifyUserGroup	Concede permissão para alterar a lista de usuários que pertencem ao grupo de usuários	Write	user*		
			usergroup*		
				aws:ResourceTag/${TagKey}	
PurchaseReservedCacheNodesOffering	Concede permissão para comprar uma oferta de nó de cache reservada	Write	reserved-instance*		elasticache:AddTagsToResource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
RebalanceSlotsInGlobalReplicationGroup	Concede permissão para executar uma operação de reequilíbrio de espaço-chave para redistribuir slots e garantir uma distribuição uniforme de chaves entre fragmentos existentes em um grupo de replicação global	Write	globalreplicationgroup*		
RebootCacheCluster	Concede permissão para reiniciar alguns nós de cache (ou todos) dentro de um grupo de replicação ou cluster de cache provisionado (modo de cluster desabilitado)	Gravar	cluster*		
				aws:ResourceTag/${TagKey}	
RemoveTagsFromResource	Concede permissão para remover tags de um ElastiCache recurso	Tags	cluster		
			parametergroup		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			replicationgroup		
			reserved-instance		
			securitygroup		
			serverlesscache		
			serverlesscachesnapshot		
			snapshot		
			subnetgroup		
			user		
			usergroup		
				aws:TagKeys aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ResetCacheParameterGroup	Concede permissão para modificar parâmetros de um grupo de parâmetros de cache de volta aos seus valores padrão	Gravar	parametergroup*		
				aws:ResourceTag/${TagKey} elasticache:CacheParameterGroupName	
RevokeCacheSecurityGroupIngress	Concede permissão para remover uma entrada EC2 de grupo de segurança de um grupo de ElastiCache segurança	Gravar	securitygroup*		
				aws:ResourceTag/${TagKey}	
StartMigration	Concede permissão para iniciar uma migração de dados do Redis hospedado na Amazon EC2 ElastiCache para o Redis	Gravar	replicationgroup*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TestFailover	Concede permissão para testar failover automático em um grupo de nós especificado em um grupo de replicação	Gravar	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	
TestMigration	Concede permissão para testar uma migração de dados do Redis hospedado na Amazon EC2 ElastiCache para o Redis	Gravar	replicationgroup*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pela Amazon ElastiCache

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
		elasticache:NumNodeGroups elasticache:ReplicasPerNodeGroup elasticache:SnapshotRetentionLimit elasticache:TransitEncryptionEnabled

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
snapshot	`arn:${Partition}:elasticache:${Region}:${Account}:snapshot:${SnapshotName}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:KmsKeyId

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
		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 recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
serverlesscachesnapshot	`arn:${Partition}:elasticache:${Region}:${Account}:serverlesscachesnapshot:${ServerlessCacheSnapshotName}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:KmsKeyId

Chaves de condição para a Amazon ElastiCache

A Amazon ElastiCache define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

> **Note**
>
> Para criar elementos de condição usando chaves de condição do tipo String, use os operadores de condição que não diferenciam maiúsculas de minúsculas StringEqualsIgnoreCase ou StringNotEqualsIgnoreCase compare uma chave com um valor de string.
> Para obter informações sobre as condições em uma política do IAM para controlar o acesso ElastiCache, consulte ElastiCache Chaves no Guia ElastiCache do usuário da Amazon.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra ações com base nas etiquetas transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra as ações com base nas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra ações com base nas chaves da etiqueta transmitidas na solicitação	ArrayOfString
elasticache:AtRestEncryptionEnabled	Filtra o acesso pelo AtRestEncryptionEnabled parâmetro presente na solicitação ou pelo valor falso padrão se o parâmetro não estiver presente	Bool
elasticache:AuthTokenEnabled	Filtra o acesso pela presença de um AuthToken parâmetro não vazio na solicitação	Bool
elasticache:AutomaticFailoverEnabled	Filtra o acesso pelo AutomaticFailoverEnabled parâmetro na solicitação	Bool
elasticache:CacheNodeType	Filtra o acesso pelo cacheNodeType parâmetro presente na solicitação. Essa chave pode ser usada para restringir quais tipos de nó de cache podem ser usados na criação de cluster ou operações de dimensionamento	String
elasticache:CacheParameterGroupName	Filtra o acesso pelo CacheParameterGroupName parâmetro na solicitação	String

Chaves de condição	Descrição	Tipo
elasticache:ClusterModeEnabled	Filtra o acesso pelo parâmetro de modo de cluster presente na solicitação. O valor padrão para criações de grupo de nó único (fragmento) é false	Bool
elasticache:DataStorageUnit	Filtra o acesso pelo CacheUsageLimits. DataStorage.Parâmetro de unidade na solicitação CreateServerlessCache and ModifyServerlessCache	String
elasticache:EngineType	Filtra o acesso pelo tipo de mecanismo presente nas solicitações de criação. Para criações de grupos de replicação, o mecanismo padrão "redis" será usado como chave se o parâmetro não estiver presente	String
elasticache:EngineVersion	Filtra o acesso pelo parâmetro engineVersion presente nas solicitações de modificação de cluster ou criação	String
elasticache:KmsKeyId	Filtra o acesso pelo ID da chave KMS	String
elasticache:MaximumDataStorage	Filtra o acesso pelo CacheUsageLimits. DataStorage.Parâmetro máximo na solicitação CreateServerlessCache and ModifyServerlessCache	Numérico
elasticache:MaximumECPUPerSecond	Filtra o acesso pelo CacheUsageLimits. ECPUPerParâmetro Second.Maximum na solicitação and CreateServerlessCache ModifyServerlessCache	Numérico
elasticache:MinimumDataStorage	Filtra o acesso pelo CacheUsageLimits. DataStorage.Parâmetro mínimo na solicitação CreateServerlessCache and ModifyServerlessCache	Numérico

Chaves de condição	Descrição	Tipo
elasticache:MinimumECPUPerSecond	Filtra o acesso pelo CacheUsageLimits. ECPUPerSegundo. Parâmetro mínimo na solicitação and CreateServerlessCache ModifyServerlessCache	Numérico
elasticache:MultiAZEnabled	Filtra o acesso por AZMode parâmetro, por vários AZEnabled parâmetros ou pelo número de zonas de disponibilidade nas quais o cluster ou grupo de replicação pode ser colocado	Bool
elasticache:NumNodeGroups	Filtra o acesso pelo NodeGroupCount parâmetro NumNodeGroups or especificado na solicitação. Essa chave pode ser usada para restringir o número de grupos de nós (fragmentos) que os clusters podem ter após a criação ou as operações de dimensionamento	Numeric
elasticache:ReplicasPerNodeGroup	Filtra o acesso pelo número de réplicas por grupo de nós (fragmentos) especificado em criações ou solicitações de dimensionamento	Numérico
elasticache:SnapshotRetentionLimit	Filtra o acesso pelo SnapshotRetentionLimit parâmetro na solicitação	Numérico
elasticache:TransitEncryptionEnabled	Filtra o acesso pelo TransitEncryptionEnabled parâmetro presente na solicitação. Para criações de grupo de replicação, o valor padrão “false” será usado como chave se o parâmetro não estiver presente	Bool
elasticache:UserAuthenticationMode	Filtra o acesso pelo UserAuthenticationMode parâmetro na solicitação	String

Ações, recursos e chaves de condição do AWS Elemental Appliances and Software

AWS O Elemental Appliances and Software (prefixo do serviço:`elemental-appliances-software`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Elemental Appliances and Software
- Tipos de recursos definidos pelo AWS Elemental Appliances and Software
- Chaves de condição do AWS Elemental Appliances and Software

Ações definidas pelo AWS Elemental Appliances and Software

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa

ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CompleteUpload [somente permissão]	Concede permissão para concluir o upload de um anexo para uma cotação ou pedido	Gravar			
CreateOrderV1 [somente permissão]	Concede permissão para criar um pedido	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateQuote [somente permissão]	Concede permissão para criar uma cota	Gravar	quote*		
GetAvsCorrectAddress [somente permissão]	Concede permissão para validar um endereço	Leitura			
GetBillingAddresses [somente permissão]	Concede permissão para listar os endereços de cobrança na Conta AWS	Leitura			
GetDeliveryAddressesV2 [somente permissão]	Concede permissão para listar os endereços de entrega na AWS Conta	Leitura			
GetOrder [somente permissão]	Concede permissão para descrever um pedido	Leitura			
GetOrdersV2 [somente permissão]	Concede permissão para listar os pedidos na AWS Conta	Leitura			
GetQuote [somente permissão]	Concede permissão para descrever uma cota	Leitura	quote*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetTaxes [somente permissão]	Concede permissão para calcular impostos para um pedido	Leitura			
ListQuotes [somente permissão]	Concede permissão para listar as cotações na AWS Conta	Lista			
StartUpload [somente permissão]	Concede permissão para iniciar o upload de um anexo para uma cotação ou pedido	Gravar			
SubmitOrderV1 [somente permissão]	Concede permissão para enviar um pedido	Gravar			
UpdateQuote [somente permissão]	Concede permissão para modificar uma cota	Gravar	quote*		

Tipos de recursos definidos pelo AWS Elemental Appliances and Software

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
quote	`arn:${Partition}:elemental-appliances-software:${Region}:${Account}:quote/${ResourceId}`	

Chaves de condição do AWS Elemental Appliances and Software

O Elemental Appliances and Software não tem chaves de contexto específicas de serviço que podem ser usadas no elemento `Condition` de instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Elemental Appliances and Software Activation Service

AWS O Elemental Appliances and Software Activation Service (prefixo do serviço:`elemental-activations`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Elemental Appliances and Software Activation Service
- Tipos de recursos definidos pelo AWS Elemental Appliances and Software Activation Service
- Chaves de condição do AWS Elemental Appliances and Software Activation Service

Ações definidas pelo AWS Elemental Appliances and Software Activation Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CompleteAccountRegistration [somente permissão]	Concede permissão para concluir o processo de registro da conta do cliente para compras de aparelhos e software da AWS Elemental	Gravar			
CompleteFileUpload [somente permissão]	Concede permissão para concluir o processo de upload de um arquivo de software para equipamentos AWS elementares e compras de software	Gravar			
ConfirmAccount [somente permissão]	Concede permissão para confirmar a propriedade de ativos	Gravar			
DownloadKickstart [somente permissão]	Concede permissão para baixar os arquivos kickstart para compras de equipamentos e AWS software Elemental	Leitura			
DownloadSoftware [somente permissão]	Concede permissão para baixar os arquivos de software para equipamentos AWS elementares e compras de software	Leitura			
GenerateLicense	Concede permissão para gerar uma licença de	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
[somente permissão]	software para uma compra de equipamentos e software AWS Elemental				
GenerateLicenses [somente permissão]	Concede permissão para gerar licenças de software para equipamentos AWS elementares e compras de software	Gravar			
GetArtifactGroupSoftwareVersions [somente permissão]	Concede permissão para descrever a versão de software de um grupo de artefatos	Leitura			
GetAsset [somente permissão]	Concede permissão para descrever um ativo	Leitura			
GetAssets [somente permissão]	Concede permissão para descrever ativos associados à conta solicitante	Leitura			
GetProductAdvisories [somente permissão]	Concede permissão para obter todas as recomendações de produtos	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSoftwareVersions [somente permissão]	Concede permissão para descrever versões de software disponíveis	Leitura			
StartFileUpload [somente permissão]	Concede permissão para iniciar o processo de upload de um arquivo de software para equipamentos AWS elementares e compras de software	Gravar			

Tipos de recursos definidos pelo AWS Elemental Appliances and Software Activation Service

AWS O Elemental Appliances and Software Activation Service não suporta a especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para permitir o acesso ao AWS Elemental Appliances and Software Activation Service, especifique `"Resource": "*"` em sua política.

Chaves de condição do AWS Elemental Appliances and Software Activation Service

O Elemental Activations não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` de instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para AWS Elemental MediaConnect

AWS O Elemental MediaConnect (prefixo do serviço:`mediaconnect`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Elemental MediaConnect
- Tipos de recursos definidos pelo AWS Elemental MediaConnect
- Chaves de condição para AWS Elemental MediaConnect

Ações definidas pelo AWS Elemental MediaConnect

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de

condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddBridgeOutputs	Concede permissão para adicionar saídas a um bridge existente	Gravar	Bridge*		
AddBridgeSources	Concede permissão para adicionar origens a um bridge existente	Gravar	Bridge*		
AddFlowMediaStreams	Concede permissão para adicionar fluxos de mídia a qualquer fluxo	Write			
AddFlowOutputs	Concede permissão para adicionar saídas a qualquer fluxo	Write			
AddFlowSources	Concede permissão para adicionar fontes a qualquer fluxo	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddFlowVpcInterfaces	Concede permissão para adicionar interfaces de VPC a qualquer fluxo	Gravar			
CreateBridge	Concede permissão para criar bridges	Gravar			
CreateFlow	Concede permissão para criar fluxos	Gravar			
CreateGateway	Concede permissão para criar gateways	Gravar			
DeleteBridge	Concede permissão para excluir bridges	Gravar	Bridge*		
DeleteFlow	Concede permissão para excluir fluxos	Gravar			
DeleteGateway	Concede permissão para excluir gateways	Gravar	Gateway*		
DeregisterGatewayInstance	Concede permissão para cancelar o registro de uma instância de gateway	Gravar	GatewayInstance*		
DescribeBridge	Concede permissão para exibir os detalhes de um bridge	Leitura	Bridge*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeFlow	Concede permissão para exibir os detalhes de um fluxo incluindo o fluxo de ARN, o nome e a zona de disponibilidade, bem como detalhes sobre a origem, as saídas e os direitos	Leitura			
DescribeFlowSourceMetadata	Concede permissão para exibir informações sobre o stream de transporte de origem e os programas do fluxo	Leitura			
DescribeFlowSourceThumbnail	Concede permissão para exibir a miniatura de origem do fluxo	Leitura			
DescribeGateway	Concede permissão para exibir os detalhes de um gateway incluindo o ARN, o nome e o CIDR, bem como detalhes sobre as redes	Leitura	Gateway*		
DescribeGatewayInstance	Concede permissão para exibir os detalhes de uma instância de gateway	Leitura	GatewayInstance*		
DescribeOffering	Concede permissão para ver os detalhes de uma oferta	Read			
DescribeReservation	Concede permissão para ver os detalhes de uma reserva	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DiscoverGatewayPollEndpoint	Concede permissão para descobrir o endpoint de consulta de gateways	Gravar			
GrantFlowEntitlements	Concede permissão para conceder direitos em qualquer fluxo	Gravar			
ListBridges	Concede permissão para exibir uma lista de bridges associados a esta conta e a um ARN especificado opcionalmente	Lista	Bridge*		
ListEntitlements	Concede permissão para exibir uma lista de todos os direitos concedidos à conta	List			
ListFlows	Concede permissão para exibir uma lista de fluxos associados a esta conta	Lista			
ListGatewayInstances	Concede permissão para exibir uma lista de instâncias associadas a este gateway	Lista	GatewayInstance*		
ListGateways	Concede permissão para exibir uma lista de gateways associados a esta conta	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListOfferings	Concede permissão para exibir uma lista de todas as ofertas que estão disponíveis para a conta no momento Região da AWS	Lista			
ListReservations	Concede permissão para exibir uma lista de todas as reservas que foram compradas pela conta no momento Região da AWS	Lista			
ListTagsForResource	Concede permissão para exibir uma lista de todas as etiquetas associadas a um recurso	Leitura			
PollGateway	Concede permissão para consultar o gateway	Gravar			
PurchaseOffering	Concede permissão para comprar uma oferta	Gravar			
RemoveBridgeOutput	Concede permissão para remover uma saída de um bridge existente	Gravar	Bridge*		
RemoveBridgeSource	Concede permissão para remover uma origem de um bridge existente	Gravar	Bridge*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RemoveFlowMediaStream	Concede permissão para remover fluxos de mídia de qualquer fluxo	Write			
RemoveFlowOutput	Concede permissão para remover saídas de qualquer fluxo	Write			
RemoveFlowSource	Concede permissão para remover fontes de qualquer fluxo	Write			
RemoveFlowVpcInterface	Concede permissão para remover interfaces de VPC de qualquer fluxo	Write			
RevokeFlowEntitlement	Concede permissão para revogar direitos em qualquer fluxo	Write			
StartFlow	Concede permissão para iniciar fluxos	Write			
StopFlow	Concede permissão para interromper fluxos	Gravar			
SubmitGatewayStateChange	Concede permissão para enviar uma alteração de estado de gateway	Gravar			
TagResource	Concede permissão para associar etiquetas a recursos	Marcação			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para remover etiquetas de recursos	Tags			
UpdateBridge	Concede permissão para atualizar bridges	Gravar	Bridge*		
UpdateBridgeOutput	Concede permissão para atualizar uma saída de um bridge existente	Gravar	Bridge*		
UpdateBridgeSource	Concede permissão para atualizar uma origem de um bridge existente	Gravar	Bridge*		
UpdateBridgeState	Concede permissão para atualizar o estado de um bridge existente	Gravar	Bridge*		
UpdateFlow	Concede permissão para atualizar fluxos	Write			
UpdateFlowEntitlement	Concede permissão para atualizar direitos em qualquer fluxo	Write			
UpdateFlowMediaStream	Concede permissão para atualizar fluxos de mídia em qualquer fluxo	Write			
UpdateFlowOutput	Concede permissão para atualizar saídas em qualquer fluxo	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateFlowSource	Concede permissão para atualizar a fonte de qualquer fluxo	Gravar			
UpdateGatewayInstance	Concede permissão para atualizar a configuração de uma instância de gateway existente	Gravar	GatewayInstance*		

Tipos de recursos definidos pelo AWS Elemental MediaConnect

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}`	

Tipos de recursos	ARN	Chaves de condição
Source	`arn:${Partition}:mediaconnect:${Region}:${Account}:source:${SourceId}:${SourceName}`	
Gateway	`arn:${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}`	

Chaves de condição para AWS Elemental MediaConnect

MediaConnect não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para AWS Elemental MediaConvert

AWS O Elemental MediaConvert (prefixo do serviço:`mediaconvert`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Elemental MediaConvert
- Tipos de recursos definidos pelo AWS Elemental MediaConvert
- Chaves de condição para AWS Elemental MediaConvert

Ações definidas pelo AWS Elemental MediaConvert

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateCertificate	Concede permissão para associar um AWS Certificate Manager (ACM) Amazon Resource Name (ARN) ao Elemental AWS MediaConvert	Gravar			
CancelJob	Concede permissão para cancelar um MediaConvert trabalho do AWS Elemental que está esperando na fila	Gravar	Job*		
CreateJob	Concede permissão para criar e enviar uma tarefa AWS Elemental MediaConvert	Gravar	JobTemplate		
			Preset		
			Queue		
				aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys mediaconvert:HttpInputsAllowed mediaconvert:HttpsInputsAllowed mediaconvert:S3InputsAllowed	
CreateJobTemplate	Concede permissão para criar um modelo de trabalho MediaConvert personalizado do AWS Elemental	Gravar	Preset		
			Queue		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreatePreset	Concede permissão para criar uma predefinição de saída MediaConvert personalizada AWS Elemental	Gravar		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateQueue	Concede permissão para criar uma fila de MediaConvert trabalhos do AWS Elemental	Gravar		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeleteJobTemplate	Concede permissão para excluir um modelo de trabalho MediaConvert personalizado do AWS Elemental	Gravar	JobTemplate*		
DeletePolicy	Concede permissão para excluir uma política AWS Elemental MediaConvert	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeletePreset	Concede permissão para excluir uma predefinição de saída MediaConvert personalizada do AWS Elemental	Gravar	Preset*		
DeleteQueue	Concede permissão para excluir uma fila de MediaConvert trabalhos do AWS Elemental	Gravar	Queue*		
DescribeEndpoints	Concede permissão para assinar o MediaConvert serviço AWS Elemental, enviando uma solicitação para um endpoint específico da conta. Todas as solicitações de transcodificação devem ser enviadas para o endpoint que o serviço retorna	Lista			
DisassociateCertificate	Concede permissão para remover uma associação entre o Amazon Resource Name (ARN) de um AWS certificado Certificate Manager (ACM) e um recurso Elemental AWS MediaConvert	Gravar			
GetJob	Concede permissão para conseguir um emprego na AWS Elemental MediaConvert	Leitura	Job*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetJobTemplate	Concede permissão para obter um modelo de MediaConvert trabalho do AWS Elemental	Leitura	JobTemplate*		
GetPolicy	Concede permissão para obter uma política AWS Elemental MediaConvert	Leitura			
GetPreset	Concede permissão para obter uma predefinição de MediaConvert saída AWS Elemental	Leitura	Preset*		
GetQueue	Concede permissão para obter uma fila de MediaConvert trabalhos do AWS Elemental	Leitura	Queue*		
ListJobTemplates	Concede permissão para listar modelos de MediaConvert trabalho do AWS Elemental	Lista			
ListJobs	Concede permissão para listar trabalhos do AWS Elemental MediaConvert	Lista	Queue		
ListPresets	Concede permissão para listar predefinições de MediaConvert saída do AWS Elemental	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListQueues	Concede permissão para listar filas de MediaConvert trabalhos do AWS Elemental	Lista			
ListTagsForResource	Concede permissão para recuperar as tags de uma MediaConvert fila, predefinição ou modelo de trabalho	Leitura	Job		
			JobTemplate		
			Preset		
			Queue		
ListVersions	Concede permissão para listar as versões do mecanismo de MediaConvert trabalho AWS Elemental	Lista			
Probe	Concede permissão para sondar um arquivo	Leitura			
PutPolicy	Concede permissão para colocar uma política AWS Elemental MediaConvert	Gravar			
SearchJobs	Concede permissão para pesquisar empregos na AWS Elemental MediaConvert	Lista	Queue		
TagResource	Concede permissão para adicionar tags a uma MediaConvert fila, predefinição ou modelo de trabalho	Tags	Job		
			JobTemplate		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			Preset		
			Queue		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover tags de uma MediaConvert fila, predefinição ou modelo de trabalho	Tags	Job		
			JobTemplate		
			Preset		
			Queue		
				aws:TagKeys	
UpdateJobTemplate	Concede permissão para atualizar um modelo de trabalho MediaConvert personalizado do AWS Elemental	Gravar	JobTemplate*		
			Preset		
			Queue		
UpdatePreset	Concede permissão para atualizar uma predefinição de saída MediaConvert personalizada do AWS Elemental	Gravar	Preset*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateQueue	Concede permissão para atualizar uma fila de MediaConvert trabalhos do AWS Elemental	Gravar	Queue*		

Tipos de recursos definidos pelo AWS Elemental MediaConvert

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Tipos de recursos	ARN	Chaves de condição
CertificateAssociation	`arn:${Partition}:mediaconvert:${Region}:${Account}:certificates/${CertificateArn}`	

Chaves de condição para AWS Elemental MediaConvert

AWS O Elemental MediaConvert define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta na solicitação	ArrayOfString
mediaconvert:HttpInputsAllowed	Filtra o acesso por uma política de entrada HTTP presente na conta	Bool
mediaconvert:HttpsInputsAllowed	Filtra o acesso por uma política de entrada HTTPS presente na conta	Bool

Chaves de condição	Descrição	Tipo
mediaconvert:S3InputsAllowed	Filtra o acesso por uma política de entrada do S3 presente na conta	Bool

Ações, recursos e chaves de condição para AWS Elemental MediaLive

AWS O Elemental MediaLive (prefixo do serviço:`medialive`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Elemental MediaLive
- Tipos de recursos definidos pelo AWS Elemental MediaLive
- Chaves de condição para AWS Elemental MediaLive

Ações definidas pelo AWS Elemental MediaLive

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o

nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptInputDeviceTransfer	Concede permissão para aceitar uma transferência de dispositivo de entrada	Write	input-device*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchDelete	Concede permissão para excluir canais, entradas, grupos de segurança de entrada e multiplexes	Write			
BatchStart	Concede permissão para iniciar canais e multiplexes	Write			
BatchStop	Concede permissão para interromper canais e multiplexes	Write			
BatchUpdateSchedule	Concede permissão para adicionar e remover ações do cronograma de um canal	Write	channel*		
CancelInputDeviceTransfer	Concede permissão para cancelar uma transferência de dispositivo de entrada	Gravar	input-device*		
ClaimDevice	Concede permissão para atualizar um dispositivo de entrada	Gravar	input-device*		
CreateChannel	Concede permissão para criar um canal	Gravar	channel*		
			input*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateChannelPlacementGroup	Concede permissão para criar um cluster.	Gravar	channel-placement-group*		
			cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudWatchAlarmTemplate	Concede permissão para criar um modelo de alarme do Cloudwatch	Gravar	cloudwatch-alarm-template*		
			cloudwatch-alarm-template-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudWatchAlarmTemplateGroup	Concede permissão para criar um grupo de modelos de alarme do Cloudwatch	Gravar	cloudwatch-alarm-template-group*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCluster	Concede permissão para criar um cluster.	Gravar	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventBridgeRuleTemplate	Concede permissão para criar um modelo de regra do Eventbridge	Gravar	eventbridge-rule-template*		
			eventbridge-rule-template-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateEventBridgeRuleTemplateGroup	Concede permissão para criar um grupo de modelos de regras do Eventbridge	Gravar	eventbridge-rule-template-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInput	Concede permissão para criar uma entrada	Write	input*		
			input-security-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInputSecurityGroup	Concede permissão para criar um grupo de segurança de entrada	Write	input-security-group*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMultiplex	Concede permissão para criar um multiplex	Write	multiplex*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMultiplexProgram	Concede permissão para criar um programa multiplex	Gravar	multiplex*		
CreateNetwork	Concede permissão para criar uma rede	Gravar	network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNode	Concede permissão para criar um nó	Gravar	cluster*		
			node*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNodeRegistrationScript	Concede permissão para criar um script de registro do nó	Gravar	cluster*		
CreatePartnerInput	Concede permissão para criar uma colaboração de parceiro	Gravar	input*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSdiSource	Concede permissão para criar uma fonte SDI	Gravar	sdi-source*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSignalMap	Concede permissão para criar um mapa de sinais	Gravar	signal-map*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTags	Concede permissão para criar tags para canais, entradas, grupos de segurança de entrada, multiplexes, reservas, nós, redes, clusters, grupos de posicionamento de canais, mapas de sinais, fontes SDI, grupos de modelos e modelos	Tags	channel		
			channel-placement-group		
			cloudwatch-alarm-template		
			cloudwatch-alarm-template-group		
			cluster		
			eventbridge-rule-template		
			eventbridge-rule-template-group		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			input		
			input-security-group		
			multiplex		
			network		
			node		
			reservation		
			sdi-source		
			signal-map		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteChannel	Concede permissão para excluir um canal	Gravar	channel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteChannelPlacementGroup	Concede permissão para excluir um cluster	Gravar	channel-placement-group*		
DeleteCloudWatchAlarmTemplate	Concede permissão para excluir um modelo de alarme do Cloudwatch	Gravar	cloudwatch-alarm-template*		
DeleteCloudWatchAlarmTemplateGroup	Concede permissão para excluir um grupo de modelos de alarme do Cloudwatch	Gravar	cloudwatch-alarm-template-group*		
DeleteCluster	Concede permissão para excluir um cluster	Gravar	cluster*		
DeleteEventBridgeRuleTemplate	Concede permissão para excluir um modelo de regra do Eventbridge	Gravar	eventbridge-rule-template*		
DeleteEventBridgeRuleTemplateGroup	Concede permissão para excluir um grupo de modelos de regras do Eventbridge	Gravar	eventbridge-rule-template-group*		
DeleteInput	Concede permissão para excluir uma entrada	Write	input*		
DeleteInputSecurityGroup	Concede permissão para excluir um grupo de segurança de entrada	Write	input-security-group*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteMultiplex	Concede permissão para excluir um multiplex.	Write	multiplex*		
DeleteMultiplexProgram	Concede permissão para excluir um programa multiplex	Gravar	multiplex*		
DeleteNetwork	Concede permissão para excluir uma rede	Gravar	network*		
DeleteNode	Concede permissão para excluir um nó	Gravar	node*		
DeleteReservation	Concede permissão para excluir uma reserva expirada	Write	reservation*		
DeleteSchedule	Concede permissão para excluir todas as ações de agendamento de um canal	Gravar	channel*		
DeleteSdiSource	Concede permissão para excluir uma fonte SDI	Gravar	sdi-source*		
DeleteSignalMap	Concede permissão para excluir um mapa de sinais	Gravar	signal-map*		
DeleteTags	Concede permissão para excluir tags de canais, entradas, grupos de segurança de entrada, multiplexes, reservas, nós, clusters, redes, grupos de posicionamento de canais, fonte SDI, mapas de sinais, grupos de modelos e modelos	Tags	channel		
			channel-placement-group		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			cloudwatch-alarm-template		
			cloudwatch-alarm-template-group		
			cluster		
			eventbridge-rule-template		
			eventbridge-rule-template-group		
			input		
			input-security-group		
			multiplex		
			network		
			node		
			reservation		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			sdi-source		
			signal-map		
				aws:TagKeys	
DescribeAccountConfiguration	Concede permissão para exibir a configuração de conta do cliente	Leitura			
DescribeChannel	Concede permissão para obter detalhes sobre um canal	Leitura	channel*		
DescribeChannelPlacementGroup	Concede permissão para descrever um grupo de posicionamento de canais	Leitura	channel-placement-group*		
DescribeCluster	Concede permissão para descrever um cluster	Leitura	cluster*		
DescribeInput	Concede permissão para descrever uma entrada	Read	input*		
DescribeInputDevice	Concede permissão para descrever um dispositivo de entrada	Read	input-device*		
DescribeInputDeviceThumbnail	Concede permissão para descrever a miniatura de um dispositivo de entrada	Read	input-device*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeInputSecurityGroup	Concede permissão para descrever um grupo de segurança de entrada	Read	input-security-group*		
DescribeMultiplex	Concede permissão para descrever um multiplex	Read	multiplex*		
DescribeMultiplexProgram	Concede permissão para descrever um programa multiplex	Leitura	multiplex*		
DescribeNetwork	Concede permissão para descrever uma rede	Leitura	network*		
DescribeNode	Concede permissão para descrever um nó	Leitura	node*		
DescribeOffering	Concede permissão para obter detalhes sobre uma oferta de reserva	Read	offering*		
DescribeReservation	Concede permissão para obter detalhes sobre uma reserva	Read	reservation*		
DescribeSchedule	Concede permissão para exibir uma lista de ações agendadas em um canal	Leitura	channel*		
DescribeSdiSource	Concede permissão para descrever uma fonte de SDI	Leitura	sdi-source*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeThumbnails	Concede permissão para exibir as miniaturas de um canal	Leitura	channel*		
GetCloudWatchAlarmTemplate	Concede permissão para obter um modelo de alarme do Cloudwatch	Leitura	cloudwatch-alarm-template*		
GetCloudWatchAlarmTemplateGroup	Concede permissão para obter um grupo de modelos de alarme do Cloudwatch	Leitura	cloudwatch-alarm-template-group*		
GetEventBridgeRuleTemplate	Concede permissão para obter um modelo de regra do Eventbridge	Leitura	eventbridge-rule-template*		
GetEventBridgeRuleTemplateGroup	Concede permissão para obter um grupo de modelos de regra do Eventbridge	Leitura	eventbridge-rule-template-group*		
GetSignalMap	Concede permissão para obter um mapa de sinais	Leitura	signal-map*		
ListChannelPlacementGroups	Concede permissão para listar grupos de posicionamento de canais	Lista			
ListChannels	Concede permissão para listar canais	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListCloudWatchAlarmTemplateGroups	Concede permissão para listar grupos de modelos de alarme do Cloudwatch	Lista			
ListCloudWatchAlarmTemplates	Concede permissão para listar modelos de alarme do Cloudwatch	Lista			
ListClusters	Concede permissão para listar clusters	Lista			
ListEventBridgeRuleTemplateGroups	Concede permissão para listar grupos de modelos de regra do Eventbridge	Lista			
ListEventBridgeRuleTemplates	Concede permissão para listar modelos de regra do Eventbridge	Lista			
ListInputDeviceTransfers	Concede permissão para listar transferências de dispositivos de entrada	List			
ListInputDevices	Concede permissão para listar dispositivos de entrada	List			
ListInputSecurityGroups	Concede permissão para listar os grupos de segurança de entrada	List			
ListInputs	Concede permissão para listar entradas	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListMultiplexPrograms	Concede permissão para listar programas multiplex	List			
ListMultiplexes	Concede permissão para listar multiplexes	Lista			
ListNetworks	Concede permissão para listar redes	Lista			
ListNodes	Concede permissão para listar nós	Lista			
ListOfferings	Concede permissão para listar as ofertas de reserva	List			
ListReservations	Concede permissão para listar reservas	Lista			
ListSdiSources	Concede permissão para listar fontes de SDI	Lista			
ListSignalMaps	Concede permissão para listar mapas de sinais	Lista			
ListTagsForResource	Concede permissão para listar tags para canais, entradas, grupos de segurança de entrada, multiplexes, reservas, nós, clusters, redes, grupos de posicionamento de canais, fontes SDI, mapas de sinais, grupos de modelos e modelos	Lista	channel		
			channel-placement-group		
			cloudwatch-alarm-template		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			cloudwatch-alarm-template-group		
			cluster		
			eventbridge-rule-template		
			eventbridge-rule-template-group		
			input		
			input-security-group		
			multiplex		
			network		
			node		
			reservation		
			sdi-source		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			signal-map		
ListVersions	Concede permissão para listar as versões disponíveis do MediaLive	Lista			
PollAnywhere	Concede permissão ao nó para sondar o cluster	Gravar			
PurchaseOffering	Concede permissão para comprar uma oferta de reserva	Gravar	offering*		
			reservation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RebootInputDevice	Concede permissão para reinicializar um dispositivo de entrada	Gravar	input-device*		
RejectInputDeviceTransfer	Concede permissão para rejeitar uma transferência de dispositivo de entrada	Gravar	input-device*		
RestartChannelPipelines	Concede permissão para reiniciar pipelines em um canal em execução	Gravar	channel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartChannel	Concede permissão para iniciar um canal	Gravar	channel*		
StartDeleteMonitorDeployment	Concede permissão para iniciar a exclusão do monitor de um mapa de sinais	Gravar	signal-map*		
StartInputDevice	Concede permissão para iniciar um dispositivo de entrada conectado a um MediaConnect fluxo	Gravar	input-device*		
StartInputDeviceMaintenanceWindow	Concede permissão para iniciar uma janela de manutenção para um dispositivo de entrada	Gravar	input-device*		
StartMonitorDeployment	Concede permissão para iniciar a implantação de um monitor de mapa de sinais	Gravar	signal-map*		
StartMultiplex	Concede permissão para iniciar um multiplex	Gravar	multiplex*		
StartUpdateSignalMap	Concede permissão para iniciar a atualização de um mapa de sinais	Gravar	signal-map*		
StopChannel	Concede permissão para interromper um canal	Gravar	channel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopInputDevice	Concede permissão para interromper um dispositivo de entrada conectado a um MediaConnect fluxo	Gravar	input-device*		
StopMultiplex	Concede permissão para interromper um multiplex	Gravar	multiplex*		
SubmitAnywhereStateChange	Concede permissão ao nó para enviar alterações de estado ao cluster	Gravar			
TransferInputDevice	Concede permissão para transferir um dispositivo de entrada	Gravar	input-device*		
UpdateAccountConfiguration	Concede permissão para atualizar a configuração de uma conta do cliente	Gravar			
UpdateChannel	Concede permissão para atualizar um canal	Write	channel*		
UpdateChannelClass	Concede permissão para atualizar a classe de um canal	Gravar	channel*		
UpdateChannelPlacementGroup	Concede permissão para atualizar um nó	Gravar	channel-placement-group*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateCloudWatchAlarmTemplate	Concede permissão para atualizar um modelo de alarme do Cloudwatch	Gravar	cloudwatch-alarm-template*		
			cloudwatch-alarm-template-group*		
UpdateCloudWatchAlarmTemplateGroup	Concede permissão para atualizar um grupo de modelos de alarme do Cloudwatch	Gravar	cloudwatch-alarm-template-group*		
UpdateCluster	Concede permissão para atualizar um cluster	Gravar	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateEventBridgeRuleTemplate	Concede permissão para atualizar um modelo de regra do Eventbridge	Gravar	eventbridge-rule-template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			eventbridge-rule-template-group*		
UpdateEventBridgeRuleTemplateGroup	Concede permissão para atualizar um grupo de modelos de regra do Eventbridge	Gravar	eventbridge-rule-template-group*		
UpdateInput	Concede permissão para atualizar uma entrada	Write	input*		
UpdateInputDevice	Concede permissão para atualizar um dispositivo de entrada	Write	input-device*		
UpdateInputSecurityGroup	Concede permissão para atualizar um grupo de segurança de entrada	Write	input-security-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateMultiplex	Concede permissão para atualizar um multiplex	Write	multiplex*		
UpdateMultiplexProgram	Concede permissão para atualizar um programa multiplex	Gravar	multiplex*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateNetwork	Concede permissão para atualizar o estado de um nó	Gravar	network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateNode	Concede permissão para atualizar um nó	Gravar	node*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateNodeState	Concede permissão para atualizar o estado de um nó	Gravar	node*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateReservation	Concede permissão para atualizar uma reserva	Gravar	reservation*		
UpdateSdiSource	Concede permissão para atualizar o estado de uma fonte sdi	Gravar	sdi-source*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	

Tipos de recursos definidos pelo AWS Elemental MediaLive

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
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}

Chaves de condição para AWS Elemental MediaLive

AWS O Elemental MediaLive define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento

Chaves de condição	Descrição	Tipo
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para AWS Elemental MediaPackage

AWS O Elemental MediaPackage (prefixo do serviço:`mediapackage`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Elemental MediaPackage
- Tipos de recursos definidos pelo AWS Elemental MediaPackage
- Chaves de condição para AWS Elemental MediaPackage

Ações definidas pelo AWS Elemental MediaPackage

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
Configure Logs	Concede permissão para configurar logs de acesso para um canal	Gravar	channels*		iam:CreateServiceLinkedRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateChannel	Concede permissão para criar um canal no AWS Elemental MediaPackage	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateHarvestJob	Concede permissão para criar um trabalho de colheita em AWS Elemental MediaPackage	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOriginEndpoint	Concede permissão para criar um endpoint no AWS Elemental MediaPackage	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Concede permissão para excluir um canal no AWS Elemental MediaPackage	Gravar	channels*		
DeleteOriginEndpoint	Concede permissão para excluir um endpoint no AWS Elemental MediaPackage	Gravar	origin_endpoints*		
DescribeChannel	Concede permissão para visualizar os detalhes de um canal no AWS Elemental MediaPackage	Leitura	channels*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeHarvestJob	Concede permissão para ver os detalhes de um trabalho de colheita no AWS Elemental MediaPackage	Leitura	harvest_jobs*		
DescribeOriginEndpoint	Concede permissão para visualizar os detalhes de um endpoint no AWS Elemental MediaPackage	Leitura	origin_endpoints*		
ListChannels	Concede permissão para visualizar uma lista de canais no AWS Elemental MediaPackage	Leitura			
ListHarvestJobs	Concede permissão para ver uma lista de trabalhos de colheita em AWS Elemental MediaPackage	Leitura			
ListOriginEndpoints	Concede permissão para visualizar uma lista de endpoints no AWS Elemental MediaPackage	Leitura			
ListTagsForResource	Concede permissão para listar as tags atribuídas a um canal ou OriginEndpoint	Leitura	channels		
			harvest_jobs		
			origin_endpoints		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RotateChannelCredentials	Concede permissão para alternar as credenciais para a primeira IngestEndpoint de um canal no Elemental AWS MediaPackage	Gravar	channels*		
RotateIngestEndpointCredentials	Concede permissão para alternar as IngestEndpoint credenciais de um canal no Elemental AWS MediaPackage	Gravar	channels*		
TagResource	Concede permissão para marcar um MediaPackage recurso	Tags	channels		
			harvest_jobs		
			origin_endpoints		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para excluir tags em um canal ou OriginEndpoint	Tags	channels		
			harvest_jobs		
			origin_endpoints		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
UpdateChannel	Concede permissão para fazer alterações em um canal no AWS Elemental MediaPackage	Gravar	channels*		
UpdateOriginEndpoint	Concede permissão para fazer alterações em um endpoint no AWS Elemental MediaPackage	Gravar	origin_endpoints*		

Tipos de recursos definidos pelo AWS Elemental MediaPackage

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
channels	`arn:${Partition}:mediapackage:${Region}:${Account}:channels/${ChannelIdentifier}`	aws:ResourceTag/${TagKey}
origin_endpoints	`arn:${Partition}:mediapackage:${Region}:${Account}:origin_endpoints/${OriginEndpointIdentifier}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
harvest_jobs	`arn:${Partition}:mediapackage:${Region}:${Account}:harvest_jobs/${HarvestJobIdentifier}`	aws:ResourceTag/${TagKey}

Chaves de condição para AWS Elemental MediaPackage

AWS O Elemental MediaPackage define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pela tag para uma MediaPackage solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por tag para um MediaPackage recurso	String
aws:TagKeys	Filtra o acesso pelas chaves de tag para um MediaPackage recurso ou solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS Elemental MediaPackage V2

AWS O Elemental MediaPackage V2 (prefixo do serviço:`mediapackagev2`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Elemental MediaPackage V2
- Tipos de recursos definidos pelo AWS Elemental MediaPackage V2
- Teclas de condição para AWS Elemental MediaPackage V2

Ações definidas pelo AWS Elemental MediaPackage V2

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelHarvestJob	Concede permissão para cancelar um trabalho de colheita	Gravar	Channel*		
			ChannelGroup*		
			HarvestJob*		
			OriginEndpoint*		
CreateChannel	Concede permissão para criar um canal em um grupo de canais	Gravar	Channel*		
			ChannelGroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateChannelGroup	Concede permissão para criar um grupo de canais	Gravar	ChannelGroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateHarvestJob	Concede permissão para criar um trabalho de colheita	Gravar	Channel*		
			ChannelGroup*		
			HarvestJob*		
			OriginEndpoint*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateOriginEndpoint	Concede permissão para criar um endpoint de origem para um canal	Gravar	Channel*		
			ChannelGroup*		
			OriginEndpoint*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Concede permissão para excluir um canal em um grupo de canais	Gravar	Channel*		
			ChannelGroup*		
DeleteChannelGroup	Concede permissão para excluir um grupo de canais	Gravar	ChannelGroup*		
DeleteChannelPolicy	Concede permissão para excluir uma política de recursos de um canal	Gravar	Channel*		
			ChannelGroup*		
			ChannelPolicy*		
DeleteOriginEndpoint	Concede permissão para excluir um endpoint de origem de um canal	Gravar	Channel*		
			ChannelGroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			OriginEndpoint*		
DeleteOriginEndpointPolicy	Concede permissão para excluir uma política de recursos de um endpoint de origem	Gravar	Channel*		
			ChannelGroup*		
			OriginEndpoint*		
			OriginEndpointPolicy*		
GetChannel	Concede permissão para recuperar detalhes de um canal em um grupo de canais	Leitura	Channel*		
			ChannelGroup*		
GetChannelGroup	Concede permissão para recuperar detalhes de um grupo de canais	Leitura	ChannelGroup*		
GetChannelPolicy	Concede permissão para recuperar uma política de recursos para um canal	Leitura	Channel*		
			ChannelGroup*		
			ChannelPolicy*		
GetHarvestJob	Concede permissão para recuperar detalhes de um trabalho de colheita	Leitura	Channel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			ChannelGroup*		
			HarvestJob*		
			OriginEndpoint*		
GetHeadObject	Concede permissão para fazer GetHeadObject solicitações para MediaPackage	Leitura	OriginEndpoint*		
GetObject	Concede permissão para fazer GetObject solicitações para MediaPackage	Leitura	OriginEndpoint*		
GetOriginEndpoint	Concede permissão para recuperar detalhes de um endpoint de origem	Leitura	Channel*		
			ChannelGroup*		
			OriginEndpoint*		
GetOriginEndpointPolicy	Concede permissão para recuperar detalhes de uma política de recursos para um endpoint de origem	Leitura	Channel*		
			ChannelGroup*		
			OriginEndpoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			OriginEndpointPolicy*		
HarvestObject	Concede permissão para fazer HarvestObject solicitações para MediaPackage	Leitura	OriginEndpoint*		
ListChannelGroups	Concede permissão para listar todos os grupos de canais para uma conta aws	Lista			
ListChannels	Concede permissão para listar todos os canais em um grupo de canais	Lista	ChannelGroup*		
ListHarvestJobs	Concede permissão para listar todos os trabalhos de colheita em um grupo de canais, canal e endpoint de origem	Lista	ChannelGroup*		
ListOriginEndpoints	Concede permissão para listar todos os endpoints de origem de um canal	Lista	Channel*		
			ChannelGroup*		
ListTagsForResource	Concede permissão para listar etiquetas para o recurso especificado	Leitura	Channel		
			ChannelGroup		
			HarvestJob		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			OriginEndpoint		
PutChannelPolicy	Concede permissão para anexar uma política de recursos para um canal	Gravar	Channel*		
			ChannelGroup*		
			ChannelPolicy*		
PutObject	Concede permissão para fazer PutObject solicitações para MediaPackage	Gravar	Channel*		
PutOriginEndpointPolicy	Concede permissão para anexar uma política de recursos a um endpoint de origem	Gravar	Channel*		
			ChannelGroup*		
			OriginEndpoint*		
			OriginEndpointPolicy*		
ResetChannelState	Concede permissão para redefinir um canal	Gravar	Channel*		
			ChannelGroup*		
ResetOriginEndpointState	Concede permissão para redefinir um endpoint de origem	Gravar	Channel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			ChannelGroup*		
			OriginEndpoint*		
TagResource	Concede permissão para adicionar etiquetas especificadas ao recurso especificado	Tags	Channel		
			ChannelGroup		
			HarvestJob		
			OriginEndpoint		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover as etiquetas especificadas do recurso especificado	Tags	Channel		
			ChannelGroup		
			HarvestJob		
			OriginEndpoint		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
UpdateChannel	Concede permissão para atualizar um canal em um grupo de canais	Gravar	Channel*		
			ChannelGroup*		
UpdateChannelGroup	Concede permissão para atualizar um grupo de canais	Gravar	ChannelGroup*		
UpdateOriginEndpoint	Concede permissão para atualizar um endpoint de origem de um canal	Gravar	Channel*		
			ChannelGroup*		
			OriginEndpoint*		

Tipos de recursos definidos pelo AWS Elemental MediaPackage V2

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
ChannelGroup	`arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}`	aws:ResourceTag/${TagKey}
ChannelPolicy	`arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}`	
Channel	`arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}`	aws:ResourceTag/${TagKey}
OriginEndpointPolicy	`arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}/originEndpoint/${OriginEndpointName}`	
OriginEndpoint	`arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}/originEndpoint/${OriginEndpointName}`	aws:ResourceTag/${TagKey}
HarvestJob	`arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}/originEndpoint/${OriginEndpointName}/harvestJob/${HarvestJobName}`	aws:ResourceTag/${TagKey}

Teclas de condição para AWS Elemental MediaPackage V2

AWS O Elemental MediaPackage V2 define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda

mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves de etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para AWS Elemental VOD MediaPackage

AWS O MediaPackage VOD elementar (prefixo do serviço:`mediapackage-vod`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Elemental VOD MediaPackage
- Tipos de recursos definidos pelo AWS Elemental VOD MediaPackage
- Chaves de condição para AWS Elemental VOD MediaPackage

Ações definidas pelo AWS Elemental VOD MediaPackage

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ConfigureLogs	Concede permissão para configurar registros de acesso de saída para um Packaging Group	Gravar	packaging-groups*		iam:CreateServiceLinkedRole
CreateAsset	Concede permissão para criar um ativo no AWS Elemental MediaPackage	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePackagingConfiguration	Concede permissão para criar uma configuração de empacotamento no AWS Elemental MediaPackage	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePackagingGroup	Concede permissão para criar um grupo de embalagens no AWS Elemental MediaPackage	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAsset	Concede permissão para excluir um ativo no AWS Elemental MediaPackage	Gravar	assets*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeletePackagingConfiguration	Concede permissão para excluir uma configuração de empacotamento no AWS Elemental MediaPackage	Gravar	packaging-configurations*		
DeletePackagingGroup	Concede permissão para excluir um grupo de pacotes no AWS Elemental MediaPackage	Gravar	packaging-groups*		
DescribeAsset	Concede permissão para visualizar os detalhes de um ativo no AWS Elemental MediaPackage	Leitura	assets*		
DescribePackagingConfiguration	Concede permissão para visualizar os detalhes de uma configuração de empacotamento no AWS Elemental MediaPackage	Leitura	packaging-configurations*		
DescribePackagingGroup	Concede permissão para visualizar os detalhes de um grupo de embalagens no AWS Elemental MediaPackage	Leitura	packaging-groups*		
ListAssets	Concede permissão para visualizar uma lista de ativos no AWS Elemental MediaPackage	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListPackagingConfigurations	Concede permissão para visualizar uma lista de configurações de empacotamento no AWS Elemental MediaPackage	Lista			
ListPackagingGroups	Concede permissão para visualizar uma lista de grupos de pacotes no AWS Elemental MediaPackage	Lista			
ListTagsForResource	Concede permissão para listar as tags atribuídas a um PackagingGroup Packaging Configuration, ou Ativo	Leitura	assets		
			packaging-configurations		
			packaging-groups		
TagResource	Concede permissão para atribuir tags a um Packaging Group, PackagingConfiguration, ou Ativo	Tags	assets		
			packaging-configurations		
			packaging-groups		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para excluir tags de um Packaging Group PackagingConfiguration, ou Ativo	Tags	assets		
			packaging-configurations		
			packaging-groups		
				aws:TagKeys	
UpdatePackagingGroup	Concede permissão para atualizar um grupo de pacotes no AWS Elemental MediaPackage	Gravar	packaging-groups*		

Tipos de recursos definidos pelo AWS Elemental VOD MediaPackage

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição para AWS Elemental VOD MediaPackage

AWS O MediaPackage VOD elementar define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base na presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra ações com base nos pares de chave-valor da etiqueta anexados ao recurso	String

Chaves de condição	Descrição	Type
aws:TagKeys	Filtra ações com base na presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para AWS Elemental MediaStore

AWS O Elemental MediaStore (prefixo do serviço:`mediastore`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Elemental MediaStore
- Tipos de recursos definidos pelo AWS Elemental MediaStore
- Chaves de condição para AWS Elemental MediaStore

Ações definidas pelo AWS Elemental MediaStore

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateContainer	Concede permissão para criar um contêiner	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteContainer	Concede permissão para excluir um contêiner	Gravar	container*		
DeleteContainerPolicy	Concede permissão para excluir a política de acesso de um contêiner	Gerenciamento de permissões	container*		
DeleteCorsPolicy	Concede permissão para excluir a política CORS de um contêiner	Gravar	container*		
DeleteLifecyclePolicy	Concede permissão para excluir a política de ciclo de vida de um contêiner	Gravar	container*		
DeleteMetricPolicy	Concede permissão para excluir a política de métricas de um contêiner	Gravar	container*		
DeleteObject	Concede permissão para excluir um objeto	Gravar	object*		
DescribeContainer	Concede permissão para recuperar detalhes de um contêiner	Lista	container*		
DescribeObject	Concede permissão para recuperar metadados de um objeto	Lista	object*		
GetContainerPolicy	Concede permissão para recuperar a política de acesso de um contêiner	Leitura	container*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetCorsPolicy	Concede permissão para recuperar a política CORS de um contêiner	Leitura	container*		
GetLifecyclePolicy	Concede permissão para recuperar a política de ciclo de vida atribuída a um contêiner	Leitura	container*		
GetMetricPolicy	Concede permissão para recuperar a política de métricas atribuída a um contêiner	Leitura	container*		
GetObject	Concede permissão para recuperar um objeto	Leitura	object*		
ListContainers	Concede permissão para recuperar uma lista de contêineres na conta atual	Lista			
ListItems	Concede permissão para recuperar uma lista de objetos e subpastas armazenados em uma pasta	Lista	folder		
ListTagsForResource	Concede permissão para listar as etiquetas de um contêiner	Leitura	container		
PutContainerPolicy	Concede permissão para criar ou substituir a política de acesso de um contêiner	Gerenciamento de permissões	container*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutCorsPolicy	Concede permissão para adicionar ou modificar a política CORS de um contêiner	Gravar	container*		
PutLifecyclePolicy	Concede permissão para adicionar ou modificar a política de ciclo de vida atribuída a um contêiner	Gravar	container*		
PutMetricPolicy	Concede permissão para adicionar ou modificar a política de métricas atribuída a um contêiner	Gravar	container*		
PutObject	Concede permissão para carregar um objeto	Gravar	object*		
StartAccessLogging	Concede permissão para iniciar o registro de acesso em um contêiner	Gravar	container*		iam:PassRole
StopAccessLogging	Concede permissão para interromper o registro de acesso em um contêiner	Gravar	container*		
TagResource	Concede permissão para adicionar etiquetas a um contêiner	Tags	container		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para remover etiquetas de um contêiner	Tags	container		
				aws:TagKeys	

Tipos de recursos definidos pelo AWS Elemental MediaStore

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}`	

Chaves de condição para AWS Elemental MediaStore

AWS O Elemental MediaStore define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para AWS Elemental MediaTailor

AWS O Elemental MediaTailor (prefixo do serviço:`mediatailor`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Elemental MediaTailor

- Tipos de recursos definidos pelo AWS Elemental MediaTailor
- Chaves de condição para AWS Elemental MediaTailor

Ações definidas pelo AWS Elemental MediaTailor

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ConfigureLogsForChannel	Concede permissões para configurar logs no canal com o nome de canal especificado	Gravar	channel*		
ConfigureLogsForPlaybackConfiguration	Concede permissão para configurar logs para uma configuração de reprodução	Gravar	playbackConfiguration*		iam:CreateServiceLinkedRole
CreateChannel	Concede permissão para criar um novo canal	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLiveSource	Concede permissão para criar uma nova fonte em tempo real no local origem com o nome do local origem especificado	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePrefetchSchedule	Concede permissão para criar uma programação de prefetch para a configuração de reprodução com o nome de	Gravar	playbackConfiguration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	configuração de reprodução especificado				
CreateProgram	Concede permissão para criar um novo programa no canal com o nome do canal especificado	Gravar			
CreateSourceLocation	Concede permissão para criar um novo local origem	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateVodSource	Concede permissão para criar uma nova fonte de VOD no local origem com o nome de local origem especificado	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Concede permissões para excluir o canal com o nome de canal especificado	Gravar	channel*		
DeleteChannelPolicy	Concede permissões para excluir a política do IAM no canal com o nome de canal especificado	Gerenciamento de permissões	channel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteLiveSource	Concede permissão para excluir a fonte em tempo real com o nome da fonte em tempo real especificada no local de origem, com o nome do local de origem especificado	Gravar	liveSource*		
DeletePlaybackConfiguration	Concede permissão para excluir a configuração de execução especificada	Gravar	playbackConfiguration*		
DeletePrefetchSchedule	Concede permissão para excluir uma programação de prefetch para uma configuração de reprodução com o nome da programação de prefetch especificado	Gravar	playbackConfiguration* prefetchSchedule*		
DeleteProgram	Concede permissão para excluir o programa com o nome de programa especificado no canal com o nome de canal especificado	Gravar	program*		
DeleteSourceLocation	Concede permissão para excluir o local origem com o nome de local origem especificado	Gravar	sourceLocation*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteVodSource	Concede permissão para excluir a fonte de VOD com o nome de fonte de VOD especificada no local origem com o nome de local origem especificado	Gravar	vodSource*		
DescribeChannel	Concede permissão para recuperar o canal com o nome de canal especificado	Leitura	channel*		
DescribeLiveSource	Concede permissão para recuperar a origem em tempo real com o nome da origem em tempo real especificada no local de origem, com o nome do local de origem especificado	Leitura	liveSource*		
DescribeProgram	Concede permissão para recuperar o programa com o nome de programa especificado no canal com o nome de canal especificado	Leitura	program*		
DescribeSourceLocation	Concede permissão para recuperar o local origem com o nome de local da fonte especificado	Leitura	sourceLocation*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeVodSource	Concede permissão para recuperar a fonte de VOD com o nome de fonte de VOD especificado no local origem com o nome de local origem especificado	Leitura	vodSource*		
GetChannelPolicy	Concede permissão para ler a política do IAM no canal com o nome de canal especificado	Leitura	channel*		
GetChannelSchedule	Concede permissão para recuperar o cronograma de programas no canal com o nome de canal especificado	Leitura	channel*		
GetPlaybackConfiguration	Concede permissão para recuperar a configuração do nome especificado	Leitura	playbackConfiguration*		
GetPrefetchSchedule	Concede permissão para recuperar a programação de prefetch para uma configuração de reprodução com o nome da programação de prefetch especificado	Leitura	playbackConfiguration* prefetchSchedule*		
ListAlerts	Concede permissão para recuperar a lista de alertas em um recurso	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListChannels	Concede permissão para recuperar a lista de canais existentes	Leitura			
ListLiveSources	Concede permissão para recuperar a lista de origens em tempo real no local origem com o nome do local de origem especificado	Leitura			
ListPlaybackConfigurations	Concede permissão para recuperar a lista de configurações disponíveis	Lista			
ListPrefetchSchedules	Concede permissão para recuperar a lista de programações de prefetch para uma configuração de reprodução	Lista	playbackConfiguration*		
ListSourceLocations	Concede permissão para recuperar a lista de locais de fonte existentes	Leitura			
ListTagsForResource	Concede permissão para listar as etiquetas atribuídas ao recurso de configuração de reprodução especificado	Leitura	channel		
			liveSource		
			playbackConfiguration		
			sourceLocation		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			vodSource		
ListVodSources	Concede permissão para recuperar o local origem com o nome do local origem especificado	Leitura			
PutChannelPolicy	Concede permissão para definir a política do IAM no canal com o nome de canal especificado	Gerenciamento de permissões	channel*		
PutPlaybackConfiguration	Concede permissão para adicionar uma nova configuração	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
StartChannel	Concede permissões para iniciar o canal com o nome de canal especificado	Gravar	channel*		
StopChannel	Concede permissões para interromper o canal com o nome de canal especificado	Gravar	channel*		
TagResource	Concede permissão para adicionar as etiquetas ao recurso de configuração da reprodução especificado	Tags	channel		
			liveSource		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			playbackConfiguration		
			sourceLocation		
			vodSource		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover as etiquetas do recurso de configuração de reprodução especificado	Tags	channel		
			liveSource		
			playbackConfiguration		
			sourceLocation		
			vodSource		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateChannel	Concede permissões para atualizar o canal com o nome de canal especificado	Gravar	channel*		
UpdateLiveSource	Concede permissão para atualizar a origem em tempo real com o nome da origem em tempo real especificada no local da origem, com o nome do local de origem especificado	Gravar	liveSource*		
UpdateProgram	Concede permissão para atualizar o programa com o nome de programa especificado no canal com o nome de canal especificado	Gravar	program*		
UpdateSourceLocation	Concede permissão para atualizar o local origem com o nome do local origem especificado	Gravar	sourceLocation*		
UpdateVodSource	Concede permissão para atualizar a fonte de VOD com o nome de fonte de VOD especificado no local origem com o nome de local origem especificado	Gravar	vodSource*		

Tipos de recursos definidos pelo AWS Elemental MediaTailor

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição para AWS Elemental MediaTailor

AWS O Elemental MediaTailor define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS Elemental Support Cases

AWS O Elemental Support Cases (prefixo do serviço:`elemental-support-cases`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Elemental Support Cases
- Tipos de recursos definidos pelo AWS Elemental Support Cases
- Chaves de condição para o AWS Elemental Support Cases

Ações definidas pelo AWS Elemental Support Cases

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de

recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddCaseComment [somente permissão]	Concede permissão para adicionar um comentário a um caso de suporte	Gravar	case*		
CheckCasePermission [somente permissão]	Concede permissão para verificar se o autor da chamada tem as permissões para executar operações de caso de suporte	Gravar			
CompleteMultipartUpload [somente permissão]	Concede permissão para concluir o upload de um arquivo com várias partes para um caso de suporte	Gravar	case*		
CreateCase [somente permissão]	Concede permissão para criar um caso de suporte	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
CreateS3CLIUploadCommand	Concede permissão para criar um comando cli para permitir	Gravar	case*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
[somente permissão]	o upload de um arquivo para um caso de suporte				
CreateS3DownloadUrl [somente permissão]	Concede permissão para baixar um arquivo de um caso de suporte	Gravar	case*		
GetCase [somente permissão]	Concede permissão para descrever um caso de suporte em sua conta	Leitura	case*		
GetCasePermission [somente permissão]	Concede permissão para verificar se o autor da chamada tem as permissões para executar operações de caso de suporte	Leitura			
GetCases [somente permissão]	Concede permissão para listar os casos de suporte na sua conta	Leitura			
GetUICache [somente permissão]	Concede permissão para recuperar dados do usuário do caso em cache para uso no console	Leitura			
ListTagsForCase [somente permissão]	Concede permissão para listar tags em um caso de suporte	Leitura	case*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartMultipartUpload [somente permissão]	Concede permissão para iniciar o upload de um arquivo com várias partes para um caso de suporte	Gravar	case*		
TagCase [somente permissão]	Concede permissão para adicionar uma tag em um caso de suporte	Tags	case*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagCase [somente permissão]	Concede permissão para remover uma etiqueta em um estojo de suporte	Tags	case*		
				aws:TagKeys	
UpdateCase [somente permissão]	Concede permissão para atualizar um caso de suporte	Gravar	case*		
UpdateCaseStatus [somente permissão]	Concede permissão para atualizar o status de um caso de suporte	Gravar	case*		
UpdateMultipartUpload [somente permissão]	Concede permissão para atualizar o upload de um arquivo com várias partes para um caso de suporte	Gravar	case*		

Tipos de recursos definidos pelo AWS Elemental Support Cases

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
case	`arn:${Partition}:elemental-support-cases::${Account}:case/${ResourceId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o AWS Elemental Support Cases

AWS O Elemental Support Cases define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves de etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS Elemental Support Content

AWS O Elemental Support Content (prefixo do serviço:`elemental-support-content`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Elemental Support Content
- Tipos de recursos definidos pelo AWS Elemental Support Content
- Chaves de condição para o AWS Elemental Support Content

Ações definidas pelo AWS Elemental Support Content

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa

ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
Query [somente permissão]	Concede permissão para pesquisar conteúdo de suporte	Leitura			

Tipos de recursos definidos pelo AWS Elemental Support Content

AWS O Elemental Support Content não suporta a especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para permitir acesso ao AWS Elemental Support Content, especifique `"Resource": "*"` em sua política.

Chaves de condição para o AWS Elemental Support Content

O Elemental Support Content não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento de instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o Amazon EMR no EKS (contêineres EMR)

O Amazon EMR no EKS (EMR Containers) (prefixo de serviço: `emr-containers`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em IAM políticas de permissão.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon EMR no EKS (contêineres EMR)
- Tipos de recursos definidos pelo Amazon EMR no EKS (EMR Containers)
- Chaves de condição para o Amazon EMR no EKS (contêineres EMR)

Ações definidas pelo Amazon EMR no EKS (contêineres EMR)

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o

nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelJobRun	Concede permissão para cancelar uma execução de trabalho	Gravar	jobRun*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateCertificate	Concede permissão para chamar o CreateCertificate método para aceitar CertificateSigningRequest e devolver o certificado assinado	Gravar			
CreateJobTemplate	Concede permissão para criar um modelo de trabalho	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateManagedEndpoint	Concede permissão para criar um endpoint gerenciado.	Gravar	virtualCluster*		
				aws:RequestTag/${TagKey} aws:TagKeys emr-containers:ExecutionRoleArn	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSecurityConfiguration	Concede permissão para criar uma configuração de segurança	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateVirtualCluster	Concede permissão para criar um cluster virtual	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteJobTemplate	Concede permissão para excluir um modelo de trabalho	Gravar	jobTemplate*		
DeleteManagedEndpoint	Concede permissão para excluir um endpoint gerenciado.	Write	managedEndpoint*		
DeleteVirtualCluster	Concede permissão para excluir um cluster virtual	Write	virtualCluster*		
DescribeJobRun	Concede permissão para descrever uma execução de trabalho	Leitura	jobRun*		
DescribeJobTemplate	Concede permissão para descrever um modelo de trabalho	Leitura	jobTemplate*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeManagedEndpoint	Concede permissão para descrever um endpoint gerenciado.	Leitura	managedEndpoint*		
DescribeSecurityConfiguration	Concede permissão para descrever uma configuração de segurança	Leitura	securityConfiguration*		
DescribeVirtualCluster	Concede permissão para descrever um cluster virtual	Leitura	virtualCluster*		
GetManagedEndpointSessionCredentials	Concede permissão para gerar um token de sessão usado para conectar a um endpoint gerenciado	Gravar	managedEndpoint*		
ListJobRuns	Concede permissão para listar execuções de trabalho associadas a um cluster virtual	Lista	virtualCluster*		
ListJobTemplates	Concede permissão para listar modelos de trabalho	Lista			
ListManagedEndpoints	Concede permissão para listar os endpoints gerenciados associados a um cluster virtual.	Lista	virtualCluster*		
ListSecurityConfigurations	Concede permissão para listar configurações de segurança	Lista			
ListTagsForResource		List	jobRun		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	Concede permissão para listar etiquetas para o recurso especificado		jobTemplate		
			managedEndpoint		
			securityConfiguration		
			virtualCluster		
ListVirtualClusters	Concede permissão para listar clusters virtuais	List			
StartJobRun	Concede permissão para iniciar uma execução de trabalho	Write	virtualCluster*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys emr-containers:ExecutionRoleArn emr-containers:JobTemplateArn	
TagResource	Concede permissão para marcar o recurso especificado	Marcação	jobRun		
			jobTemplate		
			managedEndpoint		
			securityConfiguration		
			virtualCluster		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar o recurso especificado	Marcação	jobRun		
			jobTemplate		
			managedEndpoint		
			securityConfiguration		
			virtualCluster		
				aws:TagKeys	

Tipos de recursos definidos pelo Amazon EMR no EKS (EMR Containers)

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição para o Amazon EMR no EKS (contêineres EMR)

O Amazon EMR on EKS (contêineres EMR) define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma IAM política. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelos pares de chave-valor da etiqueta presentes na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pelas chaves de etiqueta presentes na solicitação	ArrayOfString
emr-containers:ExecutionRoleArn	Filtra o acesso pelo ARN da função de execução presente na solicitação	ARN
emr-containers:JobTemplateArn	Filtra o acesso pelo arn do modelo de trabalho presente na solicitação	ARN

Ações, recursos e chaves de condição para o Amazon EMR Servereless

O Amazon EMR Serverless (prefixo de serviço: `emr-serverless`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon EMR Serverless
- Tipos de recursos definidos pelo Amazon EMR Serverless

- Chaves de condição para o Amazon EMR Serverless

Ações definidas pelo Amazon EMR Serverless

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AccessInteractiveEndpoints [somente permissão]	Concede permissão para executar workloads interativas em uma aplicação	Gravar	application*		iam:PassRole
AccessLivyEndpoints [somente permissão]	Concede permissão para executar workloads interativas no Livy Endpoint habilitado em uma aplicação do EMR Sem Servidor	Gravar	application*		iam:PassRole
AccessSystemProfileLogs [somente permissão]	Concede permissão para acessar os registros do perfil do sistema	Gravar	jobRun*		
CancelJobRun	Concede permissão para cancelar uma execução de trabalho	Gravar	jobRun*		
CreateApplication	Concede permissão para criar uma aplicação	Write		aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
DeleteApplication	Concede permissão para excluir um aplicativo	Gravar	application*		
GetApplication	Concede permissão para obter aplicação	Leitura	application*		
GetDashboardForJobRun	Concede permissão para obter o painel de execução de um trabalho	Leitura	jobRun*		
GetJobRun	Concede permissão para obter a execução de um trabalho	Leitura	jobRun*		
ListApplications	Concede permissão para listar aplicações	Lista			
ListJobRunAttempts	Concede permissão para listar as tentativas de execução de trabalho associadas a uma execução de trabalho	Lista	jobRun*		
ListJobRuns	Concede permissão para listar as execuções de trabalho associadas a uma aplicação	Lista	application*		
ListTagsForResource	Concede permissão para listar etiquetas para o recurso especificado	Leitura	application		
			jobRun		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartApplication	Concede permissão para iniciar uma aplicação	Gravar	application*		
StartJobRun	Concede permissão para iniciar uma execução de trabalho	Gravar	application*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
StopApplication	Concede permissão para interromper uma aplicação	Gravar	application*		
TagResource	Concede permissão para marcar o recurso especificado	Marcação	application		
			jobRun		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar o recurso especificado	Tags	application		
			jobRun		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
UpdateApplication	Concede permissão para atualizar uma aplicação	Gravar	application*		

Tipos de recursos definidos pelo Amazon EMR Serverless

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição para o Amazon EMR Serverless

O Amazon EMR Serverless define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais

as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para mensagens de usuário AWS final, SMS e voz V2

AWS O End User Messaging SMS and Voice V2 (prefixo do serviço:`sms-voice`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS End User Messaging, SMS e Voice V2
- Tipos de recursos definidos pelo AWS End User Messaging, SMS e Voice V2.
- Teclas de condição para mensagens de usuário AWS final, SMS e voz V2

Ações definidas pelo AWS End User Messaging, SMS e Voice V2

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateOriginationIdentity	Concede permissão para associar um número de telefone de origem ou ID do remetente a um grupo	Gravar	Pool*		
			PhoneNumber		
			SenderId		
AssociateProtectConfiguration	Concede permissão para associar uma configuração de proteção a um conjunto de configurações	Gravar	ConfigurationSet*		
			ProtectConfiguration*		
CreateConfigurationSet	Concede permissão para criar um conjunto de configurações	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
CreateEventDestination	Concede permissão para criar um destino de evento em um conjunto de configurações	Gravar	ConfigurationSet*		iam:PassRole
CreateOptOutList	Concede permissão para criar uma lista de recusa	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreatePool	Concede permissão para criar um grupo	Gravar	PhoneNumber		sms-voice:TagResource
			SenderId		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProtectConfiguration	Concede permissão para criar uma configuração de proteção	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
CreateRegistration	Concede permissão para criar um registro	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
CreateRegistrationAssociation	Concede permissão para associar um registro a um número de telefone ou a outro registro	Gravar	Registration*		
			PhoneNumber		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateRegistrationAttachment	Concede permissão para criar um anexo de registro	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
CreateRegistrationVersion	Concede permissão para criar uma versão de registro	Gravar	Registration*		
CreateVerifiedDestinationNumber	Concede permissão para criar um número de destino verificado	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
DeleteAccountDefaultProtectConfiguration	Concede permissão para excluir a configuração de proteção padrão da conta	Gravar			
DeleteConfigurationSet	Concede permissão para excluir um conjunto de configurações	Gravar	ConfigurationSet*		
DeleteDefaultMessageType	Concede permissão para excluir o tipo de mensagem padrão de um conjunto de configurações	Gravar	ConfigurationSet*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteDefaultSenderId	Concede permissão para excluir o ID do remetente padrão de um conjunto de configurações	Gravar	ConfigurationSet*		
DeleteEventDestination	Concede permissão para excluir um destino de evento de um conjunto de configuração	Gravar	ConfigurationSet*		
DeleteKeyword	Concede permissão para excluir uma palavra-chave de um grupo ou número de telefone de origem	Gravar	PhoneNumber		
			Pool		
DeleteMediaMessageSpendLimitOverride	Concede permissão para excluir uma substituição do limite mensal de gastos com mensagens de mídia da sua conta	Gravar			
DeleteOptOutList	Concede permissão para excluir uma lista de recusa	Gravar	OptOutList*		
DeleteOptedOutNumber	Concede permissão para excluir um número de telefone de destino de uma lista de recusa	Gravar	OptOutList*		
DeletePool	Concede permissão para excluir um grupo	Gravar	Pool*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteProtectConfiguration	Concede permissão para excluir uma configuração de proteção	Gravar	ProtectConfiguration*		
DeleteProtectConfigurationRuleSetNumberOverride	Concede permissão para excluir um número de telefone, substituindo uma configuração de proteção	Gravar	ProtectConfiguration*		
DeleteRegistration	Concede permissão para excluir um registro	Gravar	Registration*		
DeleteRegistrationAttachment	Concede permissão para excluir um anexo de registro	Gravar	RegistrationAttachment*		
DeleteRegistrationFieldValue	Concede permissão para excluir um valor de campo de registro opcional	Gravar	Registration*		
DeleteResourcePolicy	Concede permissão para excluir uma política de recurso	Gerenciamento de permissões	OptOutList		
			PhoneNumber		
			Pool		
			SenderId		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteTextMessageSpendLimitOverride	Concede permissão para excluir uma substituição para o limite de gastos mensais com sistema de mensagens de texto da conta	Gravar			
DeleteVerifiedDestinationNumber	Concede permissão para excluir um número de destino verificado	Gravar	VerifiedDestinationNumber*		
DeleteVoiceMessageSpendLimitOverride	Concede permissão para excluir uma substituição para o limite de gastos mensais com sistema de mensagens de voz da conta	Gravar			
DescribeAccountAttributes	Concede permissão para descrever os atributos da conta	Leitura			
DescribeAccountLimits	Concede permissão para descrever as cotas de serviço da conta	Leitura			
DescribeConfigurationSets	Concede permissão para descrever os conjuntos de configuração da conta	Leitura	ConfigurationSet		
DescribeKeywords	Concede permissão para descrever as palavras-chave de um grupo ou número de telefone de origem	Leitura	PhoneNumber		
			Pool		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeOptOutLists	Concede permissão para descrever as listas de recusa da conta	Leitura	OptOutList		
DescribeOptedOutNumbers	Concede permissão para descrever os números de telefone de destino de uma lista de recusa	Leitura	OptOutList*		
DescribePhoneNumbers	Concede permissão para descrever os números de telefone de origem da conta	Leitura	PhoneNumber		
DescribePools	Concede permissão para descrever os grupos da conta	Leitura	Pool		
DescribeProtectConfigurations	Concede permissão para descrever as configurações de proteção na sua conta	Leitura	ProtectConfiguration		
DescribeRegistrationAttachments	Concede permissão para descrever os anexos de registros em sua conta	Leitura	RegistrationAttachment		
DescribeRegistrationFieldDefinitions	Concede permissão para descrever as definições de campo para um determinado tipo de registro	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeRegistrationFieldValues	Concede permissão para descrever os valores de campo para um determinado registro	Leitura	Registration*		
DescribeRegistrationSectionDefinitions	Concede permissão para descrever as definições de seção para um determinado tipo de registro	Leitura			
DescribeRegistrationTypeDefinitions	Concede permissão para descrever os tipos de registro compatíveis com o serviço	Leitura			
DescribeRegistrationVersions	Concede permissão para descrever as versões de um determinado registro	Leitura	Registration*		
DescribeRegistrations	Concede permissão para descrever os registros em sua conta	Leitura	Registration		
DescribeSenderIds	Concede permissão para descrever o remetente IDs em sua conta	Leitura	SenderId		
DescribeSpendLimits	Concede permissão para descrever os limites de gastos mensais da conta	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeVerifiedDestinationNumbers	Concede permissão para descrever os números de destino verificados da conta	Leitura	VerifiedDestinationNumber		
DisassociateOriginationIdentity	Concede permissão para desassociar um número de telefone de origem ou ID do remetente a um grupo	Gravar	Pool*		
			PhoneNumber		
			SenderId		
DisassociateProtectConfiguration	Concede permissão para desassociar uma configuração de proteção de um conjunto de configurações	Gravar	ConfigurationSet*		
			ProtectConfiguration*		
DiscardRegistrationVersion	Concede permissão para descartar a versão mais recente de um determinado registro	Gravar	Registration*		
GetProtectConfigurationCountryRuleSet	Concede permissão para obter o conjunto de regras de país para uma configuração de proteção	Leitura	ProtectConfiguration*		
GetResourcePolicy	Concede permissão para obter uma política de recurso	Leitura	OptOutList		
			PhoneNumber		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			Pool		
			SenderId		
ListPoolOriginationIdentities	Concede permissão para listar todos os números de telefone de origem e remetentes IDs associados a um pool	Leitura	Pool*		
ListProtectConfigurationRuleSetNumberOverrides	Concede permissão para listar todas as substituições de números de telefone para uma configuração de proteção	Leitura	ProtectConfiguration*		
ListRegistrationAssociations	Concede permissão para listar todos os recursos associados a um recurso	Leitura	Registration*		
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	ConfigurationSet		
			OptOutList		
			PhoneNumber		
			Pool		
			ProtectConfiguration		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			Registration		
			RegistrationAttachment		
			SenderId		
			VerifiedDestinationNumber		
PutKeyword	Concede permissão para criar ou atualizar uma palavra-chave de um grupo ou número de telefone de origem	Gravar	PhoneNumber		
			Pool		
PutMessageFeedback	Concede permissão para enviar feedback para uma mensagem de texto, voz ou mídia	Gravar	Message*		
PutOptedOutNumber	Concede permissão para incluir um número de telefone de destino em uma lista de recusa	Gravar	OptOutList*		
PutProtectConfigurationRuleSetNumberOverride	Concede permissão para substituir um número de telefone em uma configuração de proteção	Gravar	ProtectConfiguration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutRegistrationFieldValue	Concede permissão para adicionar um valor de campo de registro	Gravar	Registration*		
PutResourcePolicy	Concede permissão para determinar uma política de recursos	Gerenciamento de permissões	OptOutList		
			PhoneNumber		
			Pool		
			SenderId		
ReleasePhoneNumber	Concede permissão para divulgar um número de telefone de origem	Gravar	PhoneNumber*		
ReleaseSenderId	Concede permissão para divulgar um ID de remetente	Gravar	SenderId*		
RequestPhoneNumber	Concede permissão para solicitar um número de telefone de origem	Gravar	Pool		sms-voice:AssociateOriginationIdentity sms-voice:TagResource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
RequestSenderId	Concede permissão para solicitar um ID de remetente não registrado	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
SendDestinationNumberVerificationCode	Concede permissão para enviar uma mensagem de texto ou voz contendo um código de verificação a um número de telefone de destino	Gravar	PhoneNumber		sms-voice:SendTextMessage sms-voice:SendVoiceMessage
			Pool		
			SenderId		
SendMediaMessage	Concede permissão para enviar uma mensagem de mídia a um número de telefone de destino	Gravar	PhoneNumber		
			Pool		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SendTextMessage	Concede permissão para enviar uma mensagem de texto a um número de telefone de destino	Gravar	PhoneNumber		
			Pool		
			SenderId		
SendVoiceMessage	Concede permissão para enviar uma mensagem de voz a um número de telefone de destino	Gravar	PhoneNumber		
			Pool		
SetAccountDefaultProtectConfiguration	Concede permissão para definir uma configuração de proteção padrão para a conta	Gravar	ProtectConfiguration*		
SetDefaultMessageFeedbackEnabled	Concede permissão para definir o feedback de mensagem padrão para um conjunto de configurações	Gravar	ConfigurationSet*		
SetDefaultMessageType	Concede permissão para definir o tipo de mensagem padrão de um conjunto de configurações	Gravar	ConfigurationSet*		
SetDefaultSenderId	Concede permissão para definir o ID do remetente padrão de um conjunto de configurações	Gravar	ConfigurationSet*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SetMediaMessageSpendLimitOverride	Concede permissão para definir uma substituição do limite mensal de gastos com mensagens de mídia da sua conta	Gravar			
SetTextMessageSpendLimitOverride	Concede permissão para definir uma substituição para o limite de gastos mensais com sistema de mensagens de texto da conta	Gravar			
SetVoiceMessageSpendLimitOverride	Concede permissão para definir uma substituição para o limite de gastos mensais com sistema de mensagens de voz da conta	Gravar			
SubmitRegistrationVersion	Concede permissão para enviar a versão mais recente de um determinado registro	Gravar	Registration*		
TagResource	Concede permissão para adicionar tags a um recurso	Marcação	ConfigurationSet		
			OptOutList		
			PhoneNumber		
			Pool		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			ProtectConfiguration		
			Registration		
			RegistrationAttachment		
			SenderId		
			VerifiedDestinationNumber		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover etiquetas de um recurso	Tags	ConfigurationSet		
			OptOutList		
			PhoneNumber		
			Pool		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			ProtectConfiguration		
			Registration		
			RegistrationAttachment		
			SenderId		
			VerifiedDestinationNumber		
				aws:TagKeys	
UpdateEventDestination	Concede permissão para atualizar o destino de um evento em um conjunto de configurações	Gravar	ConfigurationSet*		iam:PassRole
UpdatePhoneNumber	Concede permissão para atualizar a configuração de um número de telefone de origem	Gravar	PhoneNumber*		iam:PassRole
UpdatePool	Concede permissão para atualizar a configuração de um grupo	Gravar	Pool*		iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateProtectConfiguration	Concede permissão para atualizar uma configuração de proteção	Gravar	ProtectConfiguration*		
UpdateProtectConfigurationCountryRuleSet	Concede permissão para atualizar um conjunto de regras de país para uma configuração de proteção	Gravar	ProtectConfiguration*		
UpdateSenderId	Concede permissão para atualizar a configuração do ID de um remetente	Gravar	SenderId*		
VerifyDestinationNumber	Concede permissão para verificar um número de telefone de destino	Gravar	VerifiedDestinationNumber*		

Tipos de recursos definidos pelo AWS End User Messaging, SMS e Voice V2.

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}
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}

Tipos de recursos	ARN	Chaves de condição
Message	`arn:${Partition}:sms-voice:${Region}:${Account}:message/${MessageId}`	

Teclas de condição para mensagens de usuário AWS final, SMS e voz V2

AWS O End User Messaging SMS and Voice V2 define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS End User Messaging Social

AWS O End User Messaging Social (prefixo do serviço:`social-messaging`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.

- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS End User Messaging Social
- Tipos de recursos definidos pelo AWS End User Messaging Social
- Chaves de condição do AWS End User Messaging Social

Ações definidas pelo AWS End User Messaging Social

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateWhatsAppBusinessAccount	Concede permissão para associar uma conta WhatsApp comercial à sua Conta da AWS	Gravar		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateWhatsAppMessageTemplate	Concede permissão para criar um modelo de WhatsApp mensagem	Gravar			
CreateWhatsAppMessageTemplateFromLibrary	Concede permissão para criar um modelo de WhatsApp mensagem a partir da biblioteca de modelos do Meta	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateWhatsAppMessageTemplateMedia	Concede permissão para criar mídia para modelos de WhatsApp mensagens	Gravar			
DeleteWhatsAppMessageMedia	Concede permissão para excluir um objeto de mídia do WhatsApp	Gravar	phone-number-id*		
DeleteWhatsAppMessageTemplate	Concede permissão para excluir um modelo de WhatsApp mensagem	Gravar			
DisassociateWhatsAppBusinessAccount	Concede permissão para desassociar uma conta WhatsApp comercial de sua Conta da AWS	Gravar	waba*		
GetLinkedWhatsAppBusinessAccount	Concede permissão para visualizar os detalhes de uma conta WhatsApp comercial	Leitura	waba*		
GetLinkedWhatsAppBusinessAccountPhoneNumber	Concede permissão para exibir os detalhes de um número de telefone	Leitura	phone-number-id*		
GetWhatsAppMessageMedia	Concede permissão para obter um objeto de mídia de WhatsApp	Gravar	phone-number-id*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetWhatsAppMessageTemplate	Concede permissão para obter detalhes de um modelo de WhatsApp mensagem	Leitura			
ListLinkedWhatsAppBusinessAccounts	Concede permissão para visualizar todas as suas contas WhatsApp comerciais	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	phone-number-id		
			waba		
ListWhatsAppMessageTemplates	Concede permissão para listar modelos de WhatsApp mensagens	Lista			
ListWhatsAppTemplateLibrary	Concede permissão para listar os modelos disponíveis da biblioteca de modelos do Meta	Lista			
PostWhatsAppMessageMedia	Concede permissão para fazer upload de um objeto de mídia para WhatsApp	Gravar	phone-number-id*		
PutWhatsAppBusinessAccountEventDestinations	Concede permissão para atualizar o destino WhatsApp de um evento de contas comerciais	Gravar	waba*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SendWhatsAppMessage	Concede permissão para enviar uma mensagem por WhatsApp	Gravar	phone-number-id*		
TagResource	Concede permissão para adicionar uma etiqueta a um recurso	Marcação	phone-number-id		
			waba		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover uma etiqueta de um recurso	Tags	phone-number-id		
			waba		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateWhatsAppMessageTemplate	Concede permissão para atualizar um modelo de WhatsApp mensagem	Gravar			

Tipos de recursos definidos pelo AWS End User Messaging Social

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS End User Messaging Social

AWS O End User Messaging Social define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Entity Resolution

AWS A resolução de entidades (prefixo do serviço:`entityresolution`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela AWS Entity Resolution
- Tipos de recursos definidos pela AWS Entity Resolution
- Chaves de condição para AWS Entity Resolution

Ações definidas pela AWS Entity Resolution

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou

ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddPolicyStatement	Concede permissão para conceder a um AWS serviço ou outra conta permissão para usar os recursos de uma Resolução de AWS Entidades	Gerenciamento de permissões			
BatchDeleteUniqueId	Concede permissão para excluir IDs exclusivos em lote	Gravar	MatchingWorkflow*		
CreateIdMappingWorkflow	Concede permissão para criar um fluxo de trabalho de idmapping	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateIdNamespace	Concede permissão para criar um IdNamespace	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateMatchingWorkflow	Concede permissão para criar um fluxo de trabalho correspondente	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSchemaMapping	Concede permissão para criar um mapeamento de esquema	Gravar		aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
DeleteIdMappingWorkflow	Concede permissão para excluir um fluxo de trabalho de idmapping	Gravar	IdMappingWorkflow*		
DeleteIdNamespace	Concede permissão para excluir um IdNamespace	Gravar	IdNamespace*		
DeleteMatchingWorkflow	Concede permissão para excluir um fluxo de trabalho correspondente	Gravar	MatchingWorkflow*		
DeletePolicyStatement	Concede permissão para excluir a permissão concedida a um AWS serviço ou outra conta, permissão para usar os recursos de uma Resolução de AWS Entidades	Gerenciamento de permissões			
DeleteSchemaMapping	Concede permissão para excluir um mapeamento de esquema	Gravar	SchemaMapping*		
GenerateMatchId	Concede permissão para gerar ID de correspondência	Gravar	MatchingWorkflow*		
GetIdMappingJob	Concede permissão para obter um trabalho de idmapping	Leitura	IdMappingWorkflow*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetIdMappingWorkflow	Concede permissão para obter um fluxo de trabalho de idmapping	Leitura	IdMappingWorkflow*		
GetIdNamespace	Concede permissão para obter um IdNamespace	Leitura	IdNamespace*		
GetMatchId	Concede permissão para obter o ID correspondente	Leitura	MatchingWorkflow*		
GetMatchingJob	Concede permissão para obter um trabalho correspondente	Leitura	MatchingWorkflow*		
GetMatchingWorkflow	Concede permissão para obter um fluxo de trabalho correspondente	Leitura	MatchingWorkflow*		
GetPolicy	Concede permissão para obter uma política de recursos para recursos de Resolução de AWS Entidades	Leitura			
GetProviderService	Concede permissão para obter serviço do provedor	Leitura	ProviderService*		
GetSchemaMapping	Concede permissão para obter um mapeamento de esquema	Leitura	SchemaMapping*		
ListIdMappingJobs	Concede permissão para listar os trabalhos de idmapping	Lista	IdMappingWorkflow*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListIdMappingWorkflows	Concede permissão para listar fluxos de trabalho de idmapping	Lista			
ListIdNamespaces	Concede permissão para listar IdNamespaces	Lista			
ListMatchingJobs	Concede permissão para listar trabalhos correspondentes	Listar	MatchingWorkflow*		
ListMatchingWorkflows	Concede permissão para listar fluxos de trabalho correspondentes	Lista			
ListProviderServices	Concede permissão para listar o serviço de provedor	Lista			
ListSchemaMappings	Concede permissão para listar mapeamentos de esquema	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura			
PutPolicy	Concede permissão para colocar uma política de recursos para os recursos de resolução de uma AWS entidade	Gerenciamento de permissões			
StartIdMappingJob	Concede permissão para iniciar um trabalho de idmapping	Gravar	IdMappingWorkflow*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartMatchingJob	Concede permissão para iniciar um trabalho correspondente	Gravar	MatchingWorkflow*		
TagResource	Concede permissão para adicionar etiquetas a um recurso	Tags	IdMappingWorkflow		
			IdNamespace		
			MatchingWorkflow		
			ProviderService		
			SchemaMapping		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso	Tags	IdMappingWorkflow		
			IdNamespace		
			MatchingWorkflow		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			ProviderService		
			SchemaMapping		
				aws:TagKeys	
UpdateIdMappingWorkflow	Concede permissão para atualizar um fluxo de trabalho de idmapping	Gravar	IdMappingWorkflow*		
UpdateIdNamespace	Concede permissão para atualizar um IdNamespace	Gravar	IdNamespace*		
UpdateMatchingWorkflow	Concede permissão para atualizar um fluxo de trabalho correspondente	Gravar	MatchingWorkflow*		
UpdateSchemaMapping	Concede permissão para atualizar um mapeamento de esquema	Gravar	SchemaMapping*		
UseIdNamespace	Concede permissão para dar permissão para usar um AWS serviço ou outra conta IdNamespace em um fluxo de trabalho	Gerenciamento de permissões			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UseWorkflow	Concede permissão para dar permissão a um AWS serviço ou outra conta para usar o fluxo de trabalho em um IdNamespace	Gerenciamento de permissões			

Tipos de recursos definidos pela AWS Entity Resolution

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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/$`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
	`{ProviderName}/${ProviderServiceName}`	
IdNamespace	`arn:${Partition}:entityresolution:${Region}:${Account}:idnamespace/${IdNamespaceName}`	aws:ResourceTag/${TagKey}

Chaves de condição para AWS Entity Resolution

AWS A resolução de entidades define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por uma chave que está presente no pedido que o utilizador faz ao serviço de resolução de entidades	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso por uma chave da etiqueta e par de valores	String
aws:TagKeys	Filtra o acesso pela lista de todos os nomes de chaves de tag presentes no pedido que o utilizador faz ao serviço de resolução de entidades	ArrayOfString

Ações, recursos e chaves de condição para a Amazon EventBridge

A Amazon EventBridge (prefixo do serviço:`events`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon EventBridge
- Tipos de recursos definidos pela Amazon EventBridge
- Chaves de condição para a Amazon EventBridge

Ações definidas pela Amazon EventBridge

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ActivateEventSource	Concede permissão para ativar fontes de eventos de parceiros	Gravar	event-source*		
AllowVendedLogDeliveryForResource [somente permissão]	Concede permissão para configurar a entrega de registros vendidos para EventBridge	Gravar	event-bus*		
CancelReplay	Concede permissão para cancelar uma repetição	Write	replay*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateApiDestination	Concede permissão para criar um novo destino de api	Write	api-destination*		
			connection*		
CreateArchive	Concede permissão para criar um novo arquivamento	Write	archive*		
			event-bus*		
			alias		
			key		
CreateConnection	Concede permissão para criar uma nova conexão	Gravar	connection*		
CreateEndpoint	Concede permissão para criar um endpoint	Gravar	endpoint*		
				events:EventBusArn	
CreateEventBus	Concede permissão para criar barramentos de eventos	Write	event-bus*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreatePartnerEventSource	Concede permissão para criar fontes de eventos de parceiros	Write	event-source*		
DeactivateEventSource	Concede permissão para desativar fontes de eventos	Write	event-source*		
DeauthorizeConnection	Concede permissão para desautorizar uma conexão, excluindo seus segredos de autorização armazenados	Write	connection*		
DeleteApiDestination	Concede permissão para excluir um destino de api	Write	api-destination*		
DeleteArchive	Concede permissão para excluir um arquivamento	Write	archive*		
DeleteConnection	Concede permissão para excluir uma conexão	Gravar	connection*		
DeleteEndpoint	Concede permissão para excluir um endpoint	Gravar	endpoint*		
DeleteEventBus	Concede permissão para excluir barramentos de eventos	Write	event-bus*		
DeletePartnerEventSource	Concede permissão para excluir fontes de eventos de parceiros	Write	event-source*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteRule	Concede permissão para excluir regras	Write	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount events:ManagedBy	
DescribeApiDestination	Concede permissão para recuperar detalhes sobre um destino de api	Read	api-destination*		
			connection*		
DescribeArchive	Concede permissão para recuperar detalhes sobre um arquivamento	Read	archive*		
DescribeConnection	Concede permissão para recuperar detalhes sobre uma conexão	Leitura	connection*		
DescribeEndpoint	Concede permissão para conceder permissão para recuperar detalhes sobre um endpoint	Leitura	endpoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeEventBus	Concede permissão para recuperar detalhes sobre barramentos de eventos	Read	event-bus		
DescribeEventSource	Concede permissão para recuperar detalhes sobre fontes de eventos	Read	event-source*		
DescribePartnerEventSource	Concede permissão para recuperar detalhes sobre fontes de eventos de parceiros	Read	event-source*		
DescribeReplay	Concede permissão para recuperar os detalhes de uma repetição	Read	replay*		
DescribeRule	Concede permissão para recuperar detalhes sobre regras	Read	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount	
DisableRule	Concede permissão para desabilitar regras	Gravar	rule-on-custom-event-bus		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			rule-on-default-event-bus		
				events:creatorAccount events:ManagedBy	
EnableRule	Concede permissão para habilitar regras	Gravar	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount events:ManagedBy	
InvokeApiDestination [somente permissão]	Concede permissão para invocar um destino de api	Write	api-destination*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListApiDestinations	Concede permissão para recuperar uma lista de destinos da api	List			
ListArchives	Concede permissão para recuperar uma lista de arquivamentos	List			
ListConnections	Concede permissão para recuperar uma lista de conexões	Lista			
ListEndpoints	Concede permissão para recuperar uma lista de endpoints	Lista			
ListEventBuses	Concede permissão para recuperar uma lista dos barramentos de eventos na conta	Lista			
ListEventSources	Concede permissão para recuperar uma lista de fontes de eventos compartilhadas com essa conta	Lista			
ListPartnerEventSourceAccounts	Concede permissão para recuperar uma lista de Conta da AWS IDs associados a uma fonte de eventos	Lista	event-source*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListPartnerEventSources	Concede permissão para recuperar fontes de eventos de parceiros de lista	List			
ListReplays	Concede permissão para recuperar uma lista de repetições	List			
ListRuleNamesByTarget	Concede permissão para recuperar uma lista dos nomes das regras associadas a um destino	Lista			
ListRules	Concede permissão para recuperar uma lista das EventBridge regras da Amazon na conta	Lista			
ListTagsForResource	Concede permissão para recuperar uma lista de tags associadas a um recurso da Amazon EventBridge	Lista	event-bus		
			rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTargetsByRule	Concede permissão para recuperar uma lista de destinos definidos para uma regra	Lista	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount	
PutEvents	Concede permissão para enviar eventos personalizados para a Amazon EventBridge	Gravar	event-bus*		
				events:detail-type events:source events:eventBusInvocation	
PutPartnerEvents	Concede permissão para enviar eventos personalizados para a Amazon EventBridge	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutPermission	Concede permissão para usar a PutPermission ação para conceder permissão a outra pessoa Conta da AWS para colocar eventos em seu barramento de eventos padrão	Gerenciamento de permissões			
PutRule	Concede permissão para criar ou atualizar regras	Gravar	rule-on-custom-event-bus		
			rule-on-default-event-bus		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				events:detail.userIdentity.principalId events:detail-type events:source events:detail.service events:detail.eventTypeCode aws:RequestTag/${TagKey} aws:TagKeys events:creatorAccount events:ManagedBy	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutTargets	Concede permissão para adicionar destinos a uma regra	Gravar	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:TargetArn events:creatorAccount events:ManagedBy	
RemovePermission	Concede permissão para revogar a permissão de outra pessoa Conta da AWS para colocar eventos em seu ônibus de eventos padrão	Gerenciamento de permissões			
RemoveTargets	Concede permissão para remover destinos de uma regra	Gravar	rule-on-custom-event-bus		
			rule-on-default-event-bus		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				events:creatorAccount events:ManagedBy	
RetrieveConnectionCredentials [somente permissão]	Concede permissão para recuperar as credenciais de uma conexão	Gravar	connection*		
StartReplay	Concede permissão para iniciar uma repetição de um arquivamento	Gravar	archive*		
			event-bus*		
			replay*		
TagResource	Concede permissão para adicionar uma tag a um EventBridge recurso da Amazon	Tags	event-bus		
			rule-on-custom-event-bus		
			rule-on-default-event-bus		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey} events:creatorAccount	
TestEventPattern	Concede permissão para testar se um padrão de evento corresponde ao evento fornecido	Leitura			
UntagResource	Concede permissão para remover uma tag de um EventBridge recurso da Amazon	Tags	event-bus		
			rule-on-custom-event-bus		
			rule-on-default-event-bus		
				aws:TagKeys events:creatorAccount	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateApiDestination	Concede permissão para atualizar um destino de api	Write	api-destination*		
UpdateArchive	Concede permissão para atualizar um arquivamento	Write	archive*		
			alias		
			key		
UpdateConnection	Concede permissão para atualizar uma conexão	Gravar	connection*		
UpdateEndpoint	Concede permissão para atualizar um endpoint	Gravar	endpoint*		
				events:EventBusArn	
UpdateEventBus	Concede permissão para atualizar barramentos de evento	Gravar	event-bus*		

Tipos de recursos definidos pela Amazon EventBridge

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
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}`	

Chaves de condição para a Amazon EventBridge

A Amazon EventBridge define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelo conjunto permitido de valores para cada uma das etiquetas para barramento de eventos e ações de regras	String
aws:ResourceTag/${TagKey}	Filtra o acesso por etiqueta-valor associada ao recurso para barramento de eventos e ações de regra	String
aws:TagKeys	Filtra o acesso pelas etiquetas na solicitação para barramento de eventos e ações de regra	ArrayOfString

Chaves de condição	Descrição	Tipo
events:EventBusArn	Filtra o acesso pelo ARN dos barramentos de eventos que podem ser associados a um endpoint e às ações CreateEndpoint UpdateEndpoint	ArrayOfARN
events:ManagedBy	Filtra o acesso por AWS serviços. Se uma regra for criada por um AWS serviço em seu nome, o valor será o nome principal do serviço que criou a regra	String
events:TargetArn	Filtra o acesso pelo ARN de um alvo que pode ser colocado em uma regra para PutTargets ações. TargetArn não inclui DeadLetterConfigArn	ArrayOfARN
events:creatorAccount	Filtra o acesso pela conta em que a regra foi criada para ações de regra	String
events:detail-type	Filtra o acesso pela sequência literal do tipo de detalhe do evento e das ações PutEvents PutRule	String
events:detail.eventTypeCode	Filtra o acesso pela string literal para obter os detalhes. eventTypeCode campo do evento para PutRule ações	String
events:detail.service	Filtra o acesso pela string literal do campo detail.service do evento às ações PutRule	String
events:detail.userIdentity.principalId	Filtra o acesso pela string literal do campo detail.useridentity.principalid do evento às ações PutRule	String
events:eventBusInvocation	Filtra o acesso de acordo com o fato de o evento ter sido gerado por meio de API ou invocação de barramento entre contas para ações PutEvents	String

Chaves de condição	Descrição	Tipo
events:source	Filtra o acesso pelo AWS serviço ou pela fonte de eventos do AWS parceiro que gerou o evento PutEvents e PutRule as ações. Corresponde à string literal do campo de origem do evento	ArrayOfString

Ações, recursos e chaves de condição para Amazon EventBridge Pipes

O Amazon EventBridge Pipes (prefixo do serviço:`pipes`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon EventBridge Pipes
- Tipos de recursos definidos pelo Amazon EventBridge Pipes
- Chaves de condição para Amazon EventBridge Pipes

Ações definidas pela Amazon EventBridge Pipes

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o

nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreatePipe	Concede permissão para criar um pipe	Gravar	pipe*		iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeletePipe	Concede permissão para excluir um pipe	Gravar	pipe*		
				aws:ResourceTag/${TagKey}	
DescribePipe	Concede permissão para descrever um pipe	Leitura	pipe*		
				aws:ResourceTag/${TagKey}	
ListPipes	Concede permissão para listar todos os pipes na sua conta	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	pipe*		
				aws:ResourceTag/${TagKey}	
StartPipe	Concede permissão para iniciar um pipe	Gravar	pipe*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
StopPipe	Concede permissão para interromper um pipe	Gravar	pipe*		
				aws:ResourceTag/${TagKey}	
TagResource	Concede permissão para adicionar tags a um recurso	Marcação	pipe*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover etiquetas de um recurso	Tags	pipe*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdatePipe	Concede permissão para atualizar um pipe	Gravar	pipe*		iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pelo Amazon EventBridge Pipes

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
pipe	`arn:${Partition}:pipes:${Region}:${Account}:pipe/${Name}`	aws:ResourceTag/${TagKey}

Chaves de condição para Amazon EventBridge Pipes

O Amazon EventBridge Pipes define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por conjunto de valores permitido para cada uma das etiquetas	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelo valor-etiqueta associado ao recurso	String
aws:TagKeys	Filtra o acesso pela presença de etiquetas obrigatórias na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o Amazon EventBridge Scheduler

O Amazon EventBridge Scheduler (prefixo do serviço:`scheduler`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon EventBridge Scheduler
- Tipos de recursos definidos pelo Amazon EventBridge Scheduler
- Chaves de condição para o Amazon EventBridge Scheduler

Ações definidas pelo Amazon EventBridge Scheduler

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando

usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSchedule	Concede permissão para criar uma programação do Amazon EventBridge Scheduler	Gravar	schedule*		iam:PassRole
				aws:ResourceTag/${TagKey}	
CreateScheduleGroup	Concede permissão para criar um grupo de EventBridge agendamento do Amazon Scheduler	Gravar	schedule-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSchedule	Concede permissão para excluir uma programação do Amazon EventBridge Scheduler	Gravar	schedule*		
				aws:ResourceTag/${TagKey}	
DeleteScheduleGroup	Concede permissão para excluir um grupo de EventBridge agendamento do Amazon Scheduler	Gravar	schedule-group*		scheduler:DeleteSchedule
				aws:ResourceTag/${TagKey}	
GetSchedule	Concede permissão para visualizar detalhes sobre uma	Leitura	schedule*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	programação do Amazon EventBridge Scheduler			aws:ResourceTag/${TagKey}	
GetScheduleGroup	Concede permissão para visualizar detalhes sobre um grupo de EventBridge agendamento do Amazon Scheduler	Leitura	schedule-group*		
				aws:ResourceTag/${TagKey}	
ListScheduleGroups	Concede permissão para listar os grupos de EventBridge agendamento do Amazon Scheduler em sua conta	Lista			
ListSchedules	Concede permissão para listar os horários do Amazon EventBridge Scheduler em sua conta	Lista			
ListTagsForResource	Concede permissão para listas de tags para um recurso do Amazon EventBridge Scheduler	Leitura	schedule-group		
				aws:ResourceTag/${TagKey}	
TagResource	Concede permissão para marcar um recurso do Amazon EventBridge Scheduler	Tags	schedule-group*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permissão para desmarcar um recurso do Amazon EventBridge Scheduler	Tags	schedule-group*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateSchedule	Concede permissão para modificar uma programação do Amazon EventBridge Scheduler	Gravar	schedule*		iam:PassRole
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pelo Amazon EventBridge Scheduler

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso

também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
schedule-group	`arn:${Partition}:scheduler:${Region}:${Account}:schedule-group/${GroupName}`	aws:ResourceTag/${TagKey}
schedule	`arn:${Partition}:scheduler:${Region}:${Account}:schedule/${GroupName}/${ScheduleName}`	

Chaves de condição para o Amazon EventBridge Scheduler

O Amazon EventBridge Scheduler define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para Amazon EventBridge Schemas

O Amazon EventBridge Schemas (prefixo do serviço:`schemas`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon EventBridge Schemas
- Tipos de recursos definidos pelos EventBridge esquemas da Amazon
- Chaves de condição para EventBridge esquemas da Amazon

Ações definidas pela Amazon EventBridge Schemas

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDiscoverer	Concede permissão para criar um detector de esquema de eventos. Uma vez criados, seus eventos serão mapeados automaticamente em documentos de esquema correspondentes	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRegistry	Concede permissão para criar um novo registro de esquema na conta	Gravar	registry*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSchema	Concede permissão para criar um novo esquema na conta	Gravar	schema*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDiscoverer	Concede permissão para excluir detectores da conta	Gravar	discoverer*		
DeleteRegistry	Concede permissão para excluir um registro existente de sua conta	Gravar	registry*		
DeleteResourcePolicy	Concede permissão para excluir uma política baseada em recursos anexada a determinado registro	Gravar	registry*		
DeleteSchema	Concede permissão para excluir um esquema existente em sua conta	Gravar	schema*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteSchemaVersion	Concede permissão para excluir uma versão específica do esquema da conta	Gravar	schema*		
DescribeCodeBinding	Concede permissão para recuperar metadados do código gerado para um esquema específico na conta	Leitura	schema*		
DescribeDiscoverer	Concede permissão para recuperar metadados do detector em sua conta	Leitura	discoverer*		
DescribeRegistry	Concede permissão para descrever metadados de um registro existente na conta	Leitura	registry*		
DescribeSchema	Concede permissão para recuperar um esquema existente em sua conta	Leitura	schema*		
ExportSchema	Concede permissão para exportar o AWS registro ou os esquemas descobertos no formato OpenAPI 3 para formatar JSONSchema	Leitura	registry* schema*		
GetCodeBindingSource	Concede permissão para recuperar metadados do código gerado para um esquema específico na conta	Leitura	schema*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetDiscoveredSchema	Concede permissão para recuperar um esquema da lista de eventos de exemplo fornecida	Leitura			
GetResourcePolicy	Concede permissão para recuperar uma política baseada em recursos anexada a determinado registro	Leitura	registry*		
ListDiscoverers	Concede permissão para listar todas as detecções na conta	Lista	discoverer*		
ListRegistries	Concede permissão para listar todos os registros na conta	Lista	registry*		
ListSchemaVersions	Concede permissão para listar todas as versões de um esquema	Lista	schema*		
ListSchemas	Concede permissão para listar todos os esquemas	Lista	schema*		
ListTagsForResource	Concede permissão para listar etiquetas de um recurso	Leitura	discoverer		
			registry		
			schema		
PutCodeBinding	Concede permissão para gerar código para um esquema específico na conta	Gravar	schema*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutResourcePolicy	Concede permissão para anexar uma política baseada em recursos a determinado registro	Gravar	registry*		
SearchSchemas	Concede permissão para pesquisar esquemas com base em palavras-chave especificadas na conta	Lista	schema*		
StartDiscoverer	Concede permissão para iniciar o detector especificado. Uma vez iniciado, o descobridor registrará automaticamente os esquemas para eventos publicados na fonte configurada em sua conta	Gravar	discoverer*		
StopDiscoverer	Concede permissão para interromper o detector especificado. Depois de interrompido, o detector não registrará mais os esquemas para eventos publicados na fonte configurada na conta	Gravar	discoverer*		
TagResource	Concede permissão para marcar um recurso	Tags	discoverer		
			registry		
			schema		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover uma etiqueta de um recurso	Tags	discoverer		
			registry		
			schema		
				aws:TagKeys	
UpdateDiscoverer	Concede permissão para atualizar um detector existente em sua conta	Gravar	discoverer*		
UpdateRegistry	Concede permissão para atualizar metadados de um registro existente na conta	Gravar	registry*		
UpdateSchema	Concede permissão para atualizar um esquema existente na conta	Gravar	schema*		

Tipos de recursos definidos pelos EventBridge esquemas da Amazon

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso

também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
discoverer	`arn:${Partition}:schemas:${Region}:${Account}:discoverer/${DiscovererId}`	aws:ResourceTag/${TagKey}
registry	`arn:${Partition}:schemas:${Region}:${Account}:registry/${RegistryName}`	aws:ResourceTag/${TagKey}
schema	`arn:${Partition}:schemas:${Region}:${Account}:schema/${RegistryName}/${SchemaName}`	aws:ResourceTag/${TagKey}

Chaves de condição para EventBridge esquemas da Amazon

O Amazon EventBridge Schemas define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por conjunto de valores permitido para cada uma das etiquetas	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelo valor-etiqueta associado ao recurso	String

Chaves de condição	Descrição	Tipo
aws:TagKeys	Filtra o acesso pela presença de etiquetas obrigatórias na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS Fault Injection Service

AWS O Fault Injection Service (prefixo do serviço:`fis`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Fault Injection Service
- Tipos de recursos definidos pelo AWS Fault Injection Service
- Chaves de condição para o AWS Fault Injection Service

Ações definidas pelo AWS Fault Injection Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateExperimentTemplate	Concede permissão para criar um modelo de experimento AWS FIS	Gravar	action*		
			experiment-template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTargetAccountConfiguration	Concede permissão para criar uma configuração de conta de destino do AWS FIS	Gravar	experiment-template*		
DeleteExperimentTemplate	Concede permissão para excluir o modelo de experimento AWS FIS	Gravar	experiment-template*		
DeleteTargetAccountConfiguration	Concede permissão para excluir uma configuração de conta de destino do AWS FIS	Gravar	experiment-template*		
GetAction	Concede permissão para recuperar uma ação do AWS FIS	Leitura	action*		
				aws:ResourceTag/${TagKey}	
GetExperiment	Concede permissão para recuperar um experimento AWS FIS	Leitura	experiment*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetExperimentTargetAccountConfiguration	Concede permissão para recuperar uma configuração de conta de destino do AWS FIS para um AWS experimento do FIS	Leitura	experiment*		
GetExperimentTemplate	Concede permissão para recuperar um modelo de experimento AWS FIS	Leitura	experiment-template*		
				aws:ResourceTag/${TagKey}	
GetSafetyLever	Concede permissão para obter informações sobre a medida de segurança	Leitura	safety-lever*		
GetTargetAccountConfiguration	Concede permissão para recuperar uma configuração de conta de destino do AWS FIS para um modelo de experimento do AWS FIS	Leitura	experiment-template*		
GetTargetResourceType	Concede permissão para obter informações sobre o tipo de recurso especificado	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
InjectApiInternalError [somente permissão]	Concede permissão para injetar um erro interno da API no AWS serviço fornecido a partir de um experimento do FIS	Gravar	experiment*		
				fis:Service fis:Operations fis:Percentage fis:Targets	
InjectApiThrottleError [somente permissão]	Concede permissão para injetar um erro de aceleração da API no AWS serviço fornecido a partir de um experimento do FIS	Gravar	experiment*		
				fis:Service fis:Operations fis:Percentage fis:Targets	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
InjectApiUnavailableError [somente permissão]	Concede permissão para injetar um erro de API indisponível no AWS serviço fornecido a partir de um experimento do FIS	Gravar	experiment*		
				fis:Service fis:Operations fis:Percentage fis:Targets	
ListActions	Concede permissão para listar todas as ações disponíveis AWS do FIS	Lista			
ListExperimentResolvedTargets	Concede permissão para listar alvos resolvidos para experimentos AWS do FIS	Lista	experiment*		
ListExperimentTargetAccountConfigurations	Concede permissão para listar as configurações da conta de destino para experimentos do AWS FIS	Lista	experiment*		
ListExperimentTemplates	Concede permissão para listar todos os modelos de experimentos AWS FIS disponíveis	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListExperiments	Concede permissão para listar todos os experimentos AWS FIS disponíveis	Lista			
ListTagsForResource	Concede permissão para listar as tags de um recurso AWS FIS	Leitura	action		
			experiment		
			experiment-template		
ListTargetAccountConfigurations	Concede permissão para listar as configurações da conta de destino para os modelos de experimentos AWS do FIS	Lista	experiment-template*		
ListTargetResourceTypes	Concede permissão para listar os tipos de recurso	Lista			
StartExperiment	Concede permissão para realizar um experimento AWS FIS	Gravar	experiment*		iam:CreateServiceLinkedRole
			experiment-template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
StopExperiment	Concede permissão para interromper um experimento AWS do FIS	Gravar	experiment*		
TagResource	Concede permissão para marcar recursos AWS do FIS	Tags	action		
			experiment		
			experiment-template		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para desmarcar recursos do AWS FIS	Tags	action		
			experiment		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			experiment-template		
				aws:TagKeys	
UpdateExperimentTemplate	Concede permissão para atualizar o modelo de experimento AWS FIS especificado	Gravar	experiment-template*		
			action		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateSafetyLeverState	Concede permissão para atualizar o estado da medida de segurança	Gravar	safety-lever*		
UpdateTargetAccountConfiguration	Concede permissão para atualizar uma configuração de conta de destino do AWS FIS	Gravar	experiment-template*		

Tipos de recursos definidos pelo AWS Fault Injection Service

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações

identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}`	

Chaves de condição para o AWS Fault Injection Service

AWS O Fault Injection Service define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por um par de chave valor da etiqueta que é permitido na solicitação	Segmento

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso por um par de chave e valor da etiqueta de um recurso.	Segmento
aws:TagKeys	Filtra o acesso por uma lista de chaves da etiqueta que são permitidas na solicitação	ArrayOfString
fis:Operations	Filtra o acesso pela lista de operações no AWS serviço que está sendo afetado pela ação do AWS FIS	ArrayOfString
fis:Percentage	Filtra o acesso pela porcentagem de chamadas afetadas pela ação do AWS FIS	Numérico
fis:Service	Filtra o acesso pelo AWS serviço que está sendo afetado pela ação do AWS FIS	String
fis:Targets	Filtra o acesso pela lista de recursos ARNs visados pela ação AWS FIS	ArrayOfString

Ações, recursos e chaves de condição para a Amazon FinSpace

A Amazon FinSpace (prefixo do serviço:`finspace`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon FinSpace
- Tipos de recursos definidos pela Amazon FinSpace
- Chaves de condição para a Amazon FinSpace

Ações definidas pela Amazon FinSpace

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ConnectKxCluster [somente permissão]	Concede permissão para se conectar a um cluster kdb	Gravar	kxCluster*		
CreateEnvironment	Concede permissão para criar um FinSpace ambiente	Gravar	environment*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxChangeset	Concede permissão para criar um conjunto de alterações para um banco de dados kdb	Gravar	kxDatabase*		
CreateKxCluster	Concede permissão para criar um cluster em um ambiente kdb gerenciado	Gravar	kxCluster*		ec2:DescribeSubnets finspace:MountKxDatabase
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey}	
CreateKxDatabase	Concede permissão para criar um banco de dados kdb em um ambiente kdb gerenciado	Gravar	kxDatabase*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxDataview	Concede permissão para criar uma visão de dados em um ambiente kdb gerenciado	Gravar	kxDataview*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxEnvironment	Concede permissão para criar um ambiente kdb gerenciado	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxScalingGroup	Concede permissão para criar um grupo de escalabilidade em um ambiente kdb gerenciado	Gravar	kxScalingGroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxUser	Concede permissão para criar um usuário em um ambiente kdb gerenciado	Gravar	kxEnvironment*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxVolume	Concede permissão para criar um volume em um ambiente kdb gerenciado	Gravar	kxVolume*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateUser	Concede permissão para criar um FinSpace usuário	Gravar	environment*		
			user*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteEnvironment	Concede permissão para excluir um FinSpace ambiente	Gravar	environment*		
DeleteKxCluster	Concede permissão para excluir um cluster kdb	Gravar	kxCluster*		
DeleteKxClusterNode	Concede permissão para excluir um nó de um cluster kdb	Gravar	kxCluster*		
DeleteKxDatabase	Concede permissão para excluir um banco de dados kdb	Gravar	kxDatabase*		
DeleteKxDataview	Concede permissão para excluir uma visualização de dados em um ambiente kdb gerenciado	Gravar	kxDataview*		
DeleteKxEnvironment	Concede permissão para excluir um ambiente kdb gerenciado	Gravar	kxEnvironment*		
DeleteKxScalingGroup	Concede permissão para excluir um grupo de escalabilidade em um ambiente kdb gerenciado	Gravar	kxScalingGroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteKxUser	Concede permissão para excluir um usuário kdb	Gravar	kxUser*		
DeleteKxVolume	Concede permissão para excluir um volume em um ambiente kdb gerenciado	Gravar	kxVolume*		
GetEnvironment	Concede permissão para descrever um FinSpace ambiente	Leitura	environment*		
GetKxChangeset	Concede permissão para descrever um conjunto de alterações para um banco de dados kdb	Leitura	kxDatabase*		
GetKxCluster	Concede permissão para descrever um cluster em um ambiente kdb gerenciado	Leitura	kxCluster*		
GetKxConnectionString	Concede permissão para recuperar uma string de conexão para clusters kdb	Leitura	kxCluster*		finspace:ConnectKxCluster
GetKxDatabase	Concede permissão para descrever um banco de dados kdb	Leitura	kxDatabase*		
GetKxDataview	Concede permissão para descrever uma visualização de dados em um ambiente kdb gerenciado	Leitura	kxDataview*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetKxEnvironment	Concede permissão para descrever um ambiente kdb gerenciado	Leitura	kxEnvironment*		
GetKxScalingGroup	Concede permissão para descrever um grupo de escalabilidade em um ambiente kdb gerenciado	Leitura	kxScalingGroup*		
GetKxUser	Concede permissão para descrever um usuário kdb	Leitura	kxUser*		
GetKxVolume	Concede permissão para descrever um volume em um ambiente kdb gerenciado	Leitura	kxVolume*		
GetLoadSampleDataSetGroupIntoEnvironmentStatus	Concede permissão para solicitar o status do carregamento do pacote de dados de amostra	Leitura	environment*		
GetUser	Concede permissão para descrever um FinSpace usuário	Leitura	environment*		
			user*		
ListEnvironments	Concede permissão para listar FinSpace ambientes no Conta da AWS	Lista	environment*		
ListKxChangesets	Concede permissão para listar um conjunto de alterações para um banco de dados kdb	Lista	kxDatabase*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListKxClusterNodes	Concede permissão para listar nós de cluster em um ambiente kdb gerenciado	Lista	kxCluster*		
ListKxClusters	Concede permissão para listar clusters em um ambiente kdb gerenciado	Lista	kxEnvironment*		
ListKxDatabases	Concede permissão para listar bancos de dados kdb em um ambiente kdb gerenciado	Lista	kxEnvironment*		
ListKxDataviews	Concede permissão para listar visualizações de dados em um banco de dados	Lista	kxDatabase*		
ListKxEnvironments	Concede permissão para listar ambientes kdb gerenciados	Lista			
ListKxScalingGroups	Concede permissão para listar grupos de escalabilidade em um ambiente kdb gerenciado	Lista	kxEnvironment*		
ListKxUsers	Concede permissão para listar usuários em um ambiente kdb gerenciado	Lista	kxEnvironment*		
ListKxVolumes	Concede permissão para listar volumes em um ambiente kdb gerenciado	Lista	kxEnvironment*		
ListTagsForResource	Concede permissão para retornar uma lista de etiquetas de um recurso	Lista	environment*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			kxCluster*		
			kxDatabase*		
			kxDataview*		
			kxEnvironment*		
			kxScalingGroup*		
			kxUser*		
			kxVolume*		
ListUsers	Concede permissão para listar FinSpace usuários em um ambiente	Lista	environment*		
			user*		
LoadSampleDataSetGroupIntoEnvironment	Concede permissão para carregar o pacote de dados de amostra em seu ambiente FinSpace	Gravar	environment*		
MountKxDatabase [somente permissão]	Concede permissão para montar um banco de dados em um cluster kdb	Gravar	kxDatabase*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ResetUserPassword	Concede permissão para redefinir a senha de um FinSpace usuário	Gravar	environment*		
			user*		
TagResource	Concede permissão para marcar um recurso	Marcação	environment		
			kxCluster		
			kxDatabase		
			kxDataview		
			kxEnvironment		
			kxScalingGroup		
			kxUser		
			kxVolume		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para desmarcar um recurso	Tags	environment		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			kxCluster		
			kxDatabase		
			kxDataview		
			kxEnvironment		
			kxScalingGroup		
			kxUser		
			kxVolume		
				aws:TagKeys	
UpdateEnvironment	Concede permissão para atualizar um FinSpace ambiente	Gravar	environment*		
UpdateKxClusterCodeConfiguration	Concede permissão para atualizar configurações de código para um cluster em um ambiente kdb gerenciado	Gravar	kxCluster*		
UpdateKxClusterDatabases	Concede permissão para atualizar bancos de dados para um cluster em um ambiente kdb gerenciado	Gravar	kxCluster*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateKxDatabase	Concede permissão para atualizar um banco de dados kdb	Gravar	kxDatabase*		
UpdateKxDataview	Concede permissão para atualizar uma visualização de dados em um ambiente kdb gerenciado	Gravar	kxDataview*		
UpdateKxEnvironment	Concede permissão para atualizar um ambiente kdb gerenciado	Gravar	kxEnvironment*		
UpdateKxEnvironmentNetwork	Concede permissão para atualizar a rede de um ambiente kdb gerenciado	Gravar	kxEnvironment*		
UpdateKxUser	Concede permissão para atualizar um usuário kdb	Gravar	kxUser*		
UpdateKxVolume	Concede permissão para atualizar um volume em um ambiente kdb gerenciado	Gravar	kxVolume*		
UpdateUser	Concede permissão para atualizar um FinSpace usuário	Gravar	environment*		
			user*		

Tipos de recursos definidos pela Amazon FinSpace

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações

identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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/${TagKey}
kxCluster	arn:${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/${Environme	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
	`ntId}/kxDatabase/${KxDatabase}/kxDataview/${KxDataview}`	
kxVolume	`arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxVolume/${KxVolume}`	aws:ResourceTag/${TagKey}

Chaves de condição para a Amazon FinSpace

A Amazon FinSpace define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para a FinSpace API da Amazon

A FinSpace API da Amazon (prefixo do serviço:`finspace-api`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela FinSpace API da Amazon
- Tipos de recursos definidos pela FinSpace API da Amazon
- Chaves de condição para a FinSpace API da Amazon

Ações definidas pela FinSpace API da Amazon

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetProgrammaticAccessCredentials	Concede permissão para recuperar credenciais de FinSpace acesso programático	Leitura	credential*		

Tipos de recursos definidos pela FinSpace API da Amazon

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves

são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
credential	`arn:${Partition}:finspace-api:${Region}:${Account}:/credentials/programmatic`	

Chaves de condição para a FinSpace API da Amazon

FinSpace A API não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Firewall Manager

AWS O Firewall Manager (prefixo do serviço:`fms`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Firewall Manager
- Tipos de recursos definidos pelo AWS Firewall Manager
- Chaves de condição do AWS Firewall Manager

Ações definidas pelo AWS Firewall Manager

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando

usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateAdminAccount	Concede permissão para definir a conta de administrador do AWS Firewall Manager e ativa o serviço em todas as contas da organização	Gravar			
AssociateThirdPartyFirewall	Concede permissão para definir o administrador do Firewall Manager como administrador locatário de um serviço de firewall de terceiros	Gravar			
BatchAssociateResource	Concede permissão para associar recursos a um conjunto de recursos do AWS Firewall Manager	Gravar	resource-set*		
BatchDisassociateResource	Concede permissão para desassociar recursos de um conjunto de recursos do AWS Firewall Manager	Gravar	resource-set*		
DeleteAppsList	Concede permissão para excluir permanentemente uma lista de aplicativos AWS do Firewall Manager	Gravar	applications-list*		
DeleteNotificationChannel	Concede permissão para excluir uma associação do AWS Firewall Manager com a função do IAM e o tópico Amazon Simple Notification	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	Service (SNS) que é usado para notificar o administrador de FM sobre os principais eventos e erros de FM em toda a organização				
DeletePolicy	Concede permissão para excluir permanentemente uma política AWS do Firewall Manager	Gravar	policy*		
				aws:ResourceTag/${TagKey}	
DeleteProtocolsList	Concede permissão para excluir permanentemente uma lista de protocolos AWS do Firewall Manager	Gravar	protocols-list*		
DeleteResourceSet	Concede permissão para excluir permanentemente um conjunto de recursos do AWS Firewall Manager	Gravar	resource-set*		
				aws:ResourceTag/${TagKey}	
DisassociateAdminAccount	Concede permissão para desassociar a conta que foi definida como a conta de administrador do AWS Firewall Manager e desativa o serviço em todas as contas da organização	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateThirdPartyFirewall	Concede permissão para desassociar um administrador do Firewall Manager de um locatário de firewall de terceiros	Gravar			
GetAdminAccount	Concede permissão para retornar a conta do AWS Organizations associada ao AWS Firewall Manager como administradora do AWS Firewall Manager	Leitura			
GetAdminScope	Concede permissão para retornar informações sobre o escopo administrativo da conta especificada	Leitura			
GetAppsList	Concede permissão para retornar informações sobre a lista de aplicativos AWS do Firewall Manager especificada	Leitura	applications-list*		
GetComplianceDetail	Concede permissão para recuperar informações detalhadas de conformidade sobre a conta de membro especificada. Os detalhes incluem recursos que estão dentro e fora de conformidade com a política especificada	Leitura	policy*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetNotificationChannel	Concede permissão para recuperar informações sobre o tópico Amazon Simple Notification Service (SNS) usado para registrar registros de SNS do Firewall Manager AWS	Leitura			
GetPolicy	Concede permissão para recuperar informações sobre a política especificada do AWS Firewall Manager	Leitura	policy*		
GetProtectionStatus	Concede permissão para recuperar informações resumidas de ataques em nível de política no caso de um possível ataque S DDo	Leitura	policy*		
GetProtocolsList	Concede permissão para retornar informações sobre a lista de protocolos AWS do Firewall Manager especificada	Leitura	protocols-list*		
GetResourceSet	Concede permissão para recuperar informações sobre o conjunto de recursos do AWS Firewall Manager especificado	Leitura	resource-set*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetThirdPartyFirewallAssociationStatus	Concede permissão para recuperar o status de integração de uma conta de administrador do Firewall Manager para locatário de fornecedor de firewall de terceiros	Leitura			
GetViolationDetails	Concede permissão para recuperar violações de um recurso com base na política especificada do AWS Firewall Manager e Conta da AWS	Leitura	policy*		
ListAdminAccountsForOrganization	Concede permissão para retornar um AdminAccounts objeto que lista os administradores do Firewall Manager da organização que estão integrados ao Firewall Manager por Associate AdminAccount	Lista			
ListAdminsManagingAccount	Concede permissão para listar as contas que estão gerenciando a conta de membro especificada da AWS Organizations	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAppsLists	Concede permissão para retornar uma matriz de AppsListDataSummary objetos	Lista			
ListComplianceStatus	Concede permissão para recuperar uma matriz de PolicyComplianceStatus objetos na resposta. Use PolicyComplianceStatus para obter um resumo de quais contas de membros são protegidas pela política especificada	Lista	policy*		
ListDiscoveredResources	Concede permissão para recuperar uma matriz de recursos nas contas da organização que estiverem disponíveis para uso	Lista			
ListMemberAccounts	Concede permissão para recuperar uma série de ids de contas de membros se o chamador for uma conta de administrador do FMS	Lista			
ListPolicies	Concede permissão para recuperar uma matriz de PolicySummary objetos na resposta	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListProtocolsLists	Concede permissão para retornar uma matriz de ProtocolsListDataSummary objetos	Lista			
ListResourceSetResources	Concede permissão para recuperar uma matriz de recursos que estiver associada no momento a um conjunto de recursos	Lista	resource-set*		
ListResourceSets	Concede permissão para recuperar uma matriz de objetos ResourceSetSummary	Lista			
ListTagsForResource	Concede permissão para listar Etiquetas para um determinado recurso	Leitura	policy*		
ListThirdPartyFirewallFirewallPolicies	Concede permissão para recuperar uma lista de todas as políticas de firewall de terceiro associadas à conta do administrador do firewall de terceiros	Lista			
PutAdminAccount	Concede permissão para criar ou atualizar uma conta de administrador do Firewall Manager	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutAppsList	Concede permissão para criar uma lista de aplicativos do AWS Firewall Manager	Gravar	applications-list*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutNotificationChannel	Concede permissão para designar a função do IAM e o tópico do Amazon Simple Notification Service (SNS) que o AWS Firewall Manager (FM) poderia usar para notificar o administrador de FM sobre os principais eventos e erros de FM em toda a organização	Gravar			
PutPolicy	Concede permissão para criar uma política AWS do Firewall Manager	Gravar	policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutProtocolsList	Concede permissão para criar uma lista de protocolos do AWS Firewall Manager	Gravar	protocols-list*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
PutResourceSet	Concede permissão para criar um conjunto de recursos do AWS Firewall Manager	Gravar	resource-set*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Concede permissão para adicionar uma Etiqueta a um determinado recurso	Marcação	applications-list		
			policy		
			protocols-list		
			resource-set		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para remover uma Etiqueta de um determinado recurso	Marcação	applications-list		
			policy		
			protocols-list		
			resource-set		
				aws:TagKeys	

Tipos de recursos definidos pelo AWS Firewall Manager

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS Firewall Manager

AWS O Firewall Manager define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Forecast

O Amazon Forecast (prefixo do serviço: `forecast`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Forecast
- Tipos de recursos definidos pelo Amazon Forecast
- Chaves de condição do Amazon Forecast

Ações definidas pelo Amazon Forecast

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAutoPredictor	Concede permissão para criar um preditor automático	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataset	Concede permissão para criar um conjunto de dados	Write	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDatasetGroup	Concede permissão para criar um grupo de conjuntos de dados	Write	datasetGroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDatasetImportJob	Concede permissão para criar um trabalho de importação de conjunto de dados	Gravar	datasetImportJob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExplainability	Concede permissão para criar uma explicabilidade	Gravar	forecast*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExplainabilityExport	Concede permissão para criar uma exportação de explicabilidade usando um recurso de explicabilidade	Gravar	explainability*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateForecast	Concede permissão para criar uma previsão	Gravar	predictor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateForecastEndpoint [somente permissão]	Concede permissão para criar um endpoint utilizando um recurso do Preditor	Gravar	predictor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateForecastExportJob	Concede permissão para criar um trabalho de exportação de previsão usando um recurso de previsão	Gravar	forecast*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateMonitor	Concede permissão para criar um monitor utilizando um recurso do Preditor	Gravar	predictor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePredictor	Concede permissão para criar um preditor	Write	datasetGroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePredictorBacktestExportJob	Concede permissão para criar um trabalho de exportação de teste retroativo preditora usando um preditor	Gravar	predictor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWhatIfAnalysis	Concede permissão para criar uma análise hipotética	Gravar	forecast*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWhatIfForecast	Concede permissão para criar uma previsão hipotética	Gravar	whatIfAnalysis*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWhatIfForecastExport	Concede permissão para criar uma exportação de previsão hipotética usando recursos de previsão hipotética	Gravar	whatIfForecast*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDataset	Concede permissão para excluir um conjunto de dados	Write	dataset*		
DeleteDatasetGroup	Concede permissão para excluir um grupo de conjuntos de dados	Write	datasetGroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteDatasetImportJob	Concede permissão para excluir um trabalho de importação de conjunto de dados	Gravar	datasetImportJob*		
DeleteExplainability	Concede permissão para excluir uma explicabilidade	Gravar	explainability*		
DeleteExplainabilityExport	Concede permissão para excluir uma exportação de explicabilidade	Gravar	explainabilityExport*		
DeleteForecast	Concede permissão para excluir uma previsão	Gravar	forecast*		
DeleteForecastEndpoint [somente permissão]	Concede permissão para excluir um recurso de endpoint	Gravar	endpoint*		
DeleteForecastExportJob	Concede permissão para excluir um trabalho de exportação de previsão	Gravar	forecastExport*		
DeleteMonitor	Concede permissão para excluir um recurso de monitor	Gravar	monitor*		
DeletePredictor	Concede permissão para excluir um preditor	Write	predictor*		
DeletePredictorBacktestExportJob	Concede permissão para excluir um trabalho de exportação de teste retroativo de preditor	Write	predictorBacktestExportJob*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteResourceTree	Concede permissão para excluir um recurso e seus recursos-filho.	Gravar	dataset*		
			datasetGroup*		
			datasetImportJob*		
			endpoint*		
			explainability*		
			explainabilityExport*		
			forecast*		
			forecastExport*		
			monitor*		
			predictor*		
			predictorBacktestExportJob*		
			whatIfAnalysis*		
			whatIfForecast*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			whatIfForecastExport*		
DeleteWhatIfAnalysis	Concede permissão para excluir uma análise hipotética	Gravar	whatIfAnalysis*		
DeleteWhatIfForecast	Concede permissão para excluir uma previsão hipotética	Gravar	whatIfForecast*		
DeleteWhatIfForecastExport	Concede permissão para excluir uma exportação de previsão hipotética	Gravar	whatIfForecastExport*		
DescribeAutoPredictor	Concede permissão para descrever um preditor automático	Leitura	predictor*		
DescribeDataset	Concede permissão para descrever um conjunto de dados	Read	dataset*		
DescribeDatasetGroup	Concede permissão para descrever um grupo de conjuntos de dados	Read	datasetGroup*		
DescribeDatasetImportJob	Concede permissão para descrever um trabalho de importação de conjunto de dados	Leitura	datasetImportJob*		
DescribeExplainability	Concede permissão para descrever uma explicabilidade	Leitura	explainability*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeExplainabilityExport	Concede permissão para descrever uma exportação de explicabilidade	Leitura	explainabilityExport*		
DescribeForecast	Concede permissão para descrever uma previsão	Leitura	forecast*		
DescribeForecastEndpoint [somente permissão]	Concede permissão para descrever um recurso de endpoint	Leitura	endpoint*		
DescribeForecastExportJob	Concede permissão para descrever um trabalho de exportação de previsão	Leitura	forecastExport*		
DescribeMonitor	Concede permissão para descrever um recurso de monitor	Leitura	monitor*		
DescribePredictor	Concede permissão para descrever um preditor	Read	predictor*		
DescribePredictorBacktestExportJob	Concede permissão para descrever um trabalho de exportação de teste retroativo de preditor	Leitura	predictorBacktestExportJob*		
DescribeWhatIfAnalysis	Concede permissão para descrever uma análise hipotética	Leitura	whatIfAnalysis*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeWhatIfForecast	Concede permissão para descrever uma previsão hipotética	Leitura	whatIfForecast*		
DescribeWhatIfForecastExport	Concede permissão para descrever uma exportação de previsão hipotética	Leitura	whatIfForecastExport*		
GetAccuracyMetrics	Concede permissão para obter as Métricas de precisão para um preditor	Leitura	predictor*		
GetRecentForecastContext [somente permissão]	Concede permissão para obter o contexto de previsão de uma série temporal para um endpoint	Leitura	endpoint*		
InvokeForecastEndpoint [somente permissão]	Concede permissão para invocar o endpoint para obter a previsão de uma série temporal	Leitura	endpoint*		
ListDatasetGroups	Concede permissão para listar todos os grupos de conjuntos de dados	Leitura			
ListDatasetImportJobs	Concede permissão para listar todos os trabalhos de importação do conjunto de dados	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDatasets	Concede permissão para listar todos os conjuntos de dados	Leitura			
ListExplainabilities	Concede permissão para listar todas as explicabilidades	Leitura			
ListExplainabilityExports	Concede permissão para listar todas as exportações de explicabilidades	Leitura			
ListForecastExportJobs	Concede permissão para listar todos os trabalhos de exportação de previsão	Leitura			
ListForecasts	Concede permissão para listar todas as previsões	Leitura			
ListMonitorEvaluations	Concede permissão para listar todo o resultado de avaliação para um monitor	Leitura	monitor*		
ListMonitors	Concede permissão para listar todos os recursos de monitor	Leitura			
ListPredictorBacktestExportJobs	Concede permissão para listar todos os trabalhos de exportação de teste retroativo de preditor	Leitura			
ListPredictors	Concede permissão para listar todos os preditores	Leitura			
ListTagsForResource		Leitura	dataset		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	Concede permissão para listar as etiquetas de um recurso do Amazon Forecast		datasetGroup		
			datasetImportJob		
			endpoint		
			explainability		
			explainabilityExport		
			forecast		
			forecastExport		
			monitor		
			predictor		
			predictorBacktestExportJob		
			whatIfAnalysis		
			whatIfForecast		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			whatIfForecastExport		
ListWhatIfAnalyses	Concede permissão para listar todas as análises hipotéticas	Leitura			
ListWhatIfForecastExports	Concede permissão para listar todas as exportações de previsão hipotética	Leitura			
ListWhatIfForecasts	Concede permissão para listar todas as previsões hipotéticas	Leitura			
QueryForecast	Concede permissão para recuperar uma previsão para um único item	Leitura	forecast*		
QueryWhatIfForecast	Concede permissão para recuperar uma previsão hipotética para um único item	Leitura	whatIfForecast*		
ResumeResource	Concede permissão para retomar trabalhos de recursos do Amazon Forecast	Gravar	monitor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StopResource	Concede permissão para interromper trabalhos de recursos do Amazon Forecast	Write	datasetImportJob*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			endpoint*		
			explainability*		
			explainabilityExport*		
			forecast*		
			forecastExport*		
			monitor*		
			predictor*		
			predictorBacktestExportJob*		
			whatIfAnalysis*		
			whatIfForecast*		
			whatIfForecastExport*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Concede permissão para associar as etiquetas especificadas a um recurso	Marcação	dataset		
			datasetGroup		
			datasetImportJob		
			endpoint		
			explainability		
			explainabilityExport		
			forecast		
			forecastExport		
			monitor		
			predictor		
			predictorBacktestExportJob		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			whatIfAnalysis		
			whatIfForecast		
			whatIfForecastExport		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para excluir as etiquetas especificadas para um recurso	Marcação	dataset		
			datasetGroup		
			datasetImportJob		
			endpoint		
			explainability		
			explainabilityExport		
			forecast		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			forecastExport		
			monitor		
			predictor		
			predictorBacktestExportJob		
			whatIfAnalysis		
			whatIfForecast		
			whatIfForecastExport		
				aws:TagKeys	
UpdateDatasetGroup	Concede permissão para atualizar um grupo de conjuntos de dados	Write	dataset*		
			datasetGroup*		

Tipos de recursos definidos pelo Amazon Forecast

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso

também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
dataset	`arn:${Partition}:forecast:${Region}:${Account}:dataset/${ResourceId}`	aws:ResourceTag/${TagKey}
datasetGroup	`arn:${Partition}:forecast:${Region}:${Account}:dataset-group/${ResourceId}`	aws:ResourceTag/${TagKey}
datasetImportJob	`arn:${Partition}:forecast:${Region}:${Account}:dataset-import-job/${ResourceId}`	aws:ResourceTag/${TagKey}
algorithm	`arn:${Partition}:forecast:::algorithm/${ResourceId}`	
predictor	`arn:${Partition}:forecast:${Region}:${Account}:predictor/${ResourceId}`	aws:ResourceTag/${TagKey}
predictorBacktestExportJob	`arn:${Partition}:forecast:${Region}:${Account}:predictor-backtest-export-job/${ResourceId}`	aws:ResourceTag/${TagKey}
forecast	`arn:${Partition}:forecast:${Region}:${Account}:forecast/${ResourceId}`	aws:ResourceTag/${TagKey}
forecastExport	`arn:${Partition}:forecast:${Region}:${Account}:forecast-export-job/${ResourceId}`	aws:ResourceTag/${TagKey}
explainability	`arn:${Partition}:forecast:${Region}:${Account}:explainability/${ResourceId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
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}
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}

Chaves de condição do Amazon Forecast

O Amazon Forecast define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Fraud Detector

O Amazon Fraud Detector (prefixo do serviço: `frauddetector`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Fraud Detector
- Tipos de recursos definidos pelo Amazon Fraud Detector
- Chaves de condição do Amazon Fraud Detector

Ações definidas pelo Amazon Fraud Detector

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou

ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchCreateVariable	Concede permissão para criar um lote de variáveis	Write		aws:RequestTag/${TagKey} aws:TagKeys	
BatchGetVariable	Concede permissão para obter um lote de variáveis	Lista	variable*		
CancelBatchImportJob	Concede permissão para cancelar o trabalho de importação em lote especificado	Gravar	batch-import*		
CancelBatchPredictionJob	Concede permissão para cancelar a tarefa de previsão em lote especificado	Gravar	batch-prediction*		
CreateBatchImportJob	Concede permissão para criar um trabalho de importação em lote	Gravar	batch-import*		
			event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateBatchPredictionJob	Concede permissão para criar uma tarefa de previsão em lote	Write	batch-prediction*		
			detector*		
			detector-version*		
			event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDetectorVersion	Concede permissão para criar uma versão de detector. A versão do detector é iniciada com status DRAFT.	Gravar	detector*		
			external-model		
			model-version		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateList	Concede permissão para criar uma lista	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateModel	Concede permissão para criar um modelo usando o tipo de modelo especificado	Write	event-type*		
			model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelVersion	Concede permissão para criar uma versão do modelo usando o tipo de modelo especificado e o ID do modelo	Write	model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRule	Concede permissão para criar uma regra para uso com o detector especificado	Write	detector*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVariable	Concede permissão para criar uma variável	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBatchImportJob	Concede permissão para excluir um trabalho de importação em lote	Gravar	batch-import*		
DeleteBatchPredictionJob	Concede permissão para excluir uma tarefa de previsão em lote	Write	batch-prediction*		
DeleteDetector	Concede permissão para excluir o detector. Antes de excluir um detector, você deve excluir todas as versões do detector e versões de regras associadas a ele	Write	detector*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteDetectorVersion	Concede permissão para excluir a versão do detector. Você não pode excluir versões do detector que estão no status ACTIVE.	Write	detector-version*		
DeleteEntityType	Concede permissão para excluir um tipo de entidade. Não é possível excluir um tipo de entidade incluído em um tipo de evento	Write	entity-type*		
DeleteEvent	Concede permissão para excluir o evento especificado	Write	event-type*		
DeleteEventType	Concede permissão para excluir um tipo de evento Não é possível excluir um tipo de evento que seja usado em um detector ou em um modelo	Gravar	event-type*		
DeleteEventsByEventType	Concede permissão para excluir os eventos para o tipo de evento especificado	Gravar	event-type*		
DeleteExternalModel	Concede permissão para remover um SageMaker modelo do Amazon Fraud Detector. Você pode remover um SageMaker modelo da Amazon se ele não estiver associado a uma versão do detector	Gravar	external-model*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteLabel	Concede permissão para excluir um rótulo. Não é possível excluir rótulos incluídos em um tipo de evento no Amazon Fraud Detector. Não é possível excluir um rótulo atribuído a um ID de evento. Você deve primeiro excluir o ID de evento relevante	Gravar	label*		
DeleteList	Concede permissão para excluir uma lista	Gravar	list*		
				aws:ResourceTag/${TagKey}	
DeleteModel	Concede permissão para excluir um modelo. Você pode excluir modelos e versões de modelos no Amazon Fraud Detector, desde que eles não estejam associados a uma versão do detector	Write	model*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteModelVersion	Concede permissão para excluir uma versão de modelo. Você pode excluir modelos e versões de modelos no Amazon Fraud Detector, desde que eles não estejam associados a uma versão do detector	Write	model-version*		
DeleteOutcome	Concede permissão para excluir um resultado. Não é possível excluir um resultado usado em uma versão de regra	Write	outcome*		
DeleteRule	Concede permissão para excluir a regra. Não será possível excluir uma regra se ela for usada por uma versão do detector ACTIVE ou INACTIVE	Write	rule*		
DeleteVariable	Concede permissão para excluir uma variável. Não é possível excluir variáveis incluídas em um tipo de evento no Amazon Fraud Detector.	Write	variable*		
DescribeDetector	Concede permissão para obter todas as versões do detector especificado	Read	detector*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeModelVersions	Concede permissão para obter todas as versões do modelo do tipo de modelo especificado ou do tipo e ID do modelo especificado. Você também pode obter detalhes de uma única versão do modelo especificado	Leitura	model-version		
GetBatchImportJobValidationReport [somente permissão]	Concede permissão para obter o relatório de validação de dados de um trabalho de importação de lotes específico	Leitura	batch-import*		
GetBatchImportJobs	Concede permissão para obter todas as tarefas de importação em lote ou uma tarefa específica se você especificar um ID do trabalho	Lista	batch-import		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetBatchPredictionJobs	Concede permissão para obter todas as tarefas de previsão em lote ou uma tarefa específica se você especificar um ID de tarefa. Esta é uma API paginada. Se você fornecer um maxResults nulo, essa ação recuperará um máximo de 50 registros por página. Se você fornecer um maxResults, o valor deverá estar entre 1 e 50. Para obter os resultados da próxima página, forneça o token de paginação do GetBatchPredictionJobsResponse como parte de sua solicitação. Um token de paginação nulo busca os registros desde o início	Lista	batch-prediction		
GetDeleteEventsByEventTypeStatus	Concede permissão para obter o status de execução da DeleteEventsByEventType API de um tipo de evento específico	Leitura	event-type*		
GetDetectorVersion	Concede permissão para obter uma versão específica do detector	Leitura	detector-version*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetDetectors	Concede permissão para obter todos os detectores ou um único detector se um detectorId for especificado. Esta é uma API paginada. Se você fornecer um maxResults nulo, essa ação recuperará no máximo 10 registros por página. Se você fornecer um maxResults, o valor deverá estar entre 5 e 10. Para obter os resultados da próxima página, forneça o token de paginação do GetDetectorsResponse como parte de sua solicitação. Um token de paginação nulo busca os registros desde o início	List	detector		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetEntityTypes	Concede permissão para obter todos os tipos de entidade ou um tipo de entidade específico se um nome for especificado. Esta é uma API paginada. Se você fornecer um maxResults nulo, essa ação recuperará no máximo 10 registros por página. Se você fornecer um maxResults, o valor deverá estar entre 5 e 10. Para obter os resultados da próxima página, forneça o token de paginação do GetEntityTypesResponse como parte de sua solicitação. Um token de paginação nulo busca os registros desde o início	Lista	entity-type		
GetEvent	Concede permissão para obter os detalhes do evento específico	Leitura	event-type*		
GetEventPrediction	Concede permissão para avaliar um evento em relação a uma versão do detector. Se um ID da versão não for fornecido, a versão (ACTIVE) do detector será usada	Leitura	detector*		
			detector-version*		
			event-type*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetEventPrediction Metadata	Concede permissão para obter mais detalhes de uma previsão específica	Leitura	detector*		
			detector-version*		
			event-type*		
GetEventTypes	Concede permissão para obter todos os tipos de evento ou um tipo de evento específico se o nome for fornecido. Esta é uma API paginada. Se você fornecer um maxResults nulo, essa ação recuperará no máximo 10 registros por página. Se você fornecer um maxResults, o valor deverá estar entre 5 e 10. Para obter os resultados da próxima página, forneça o token de paginação do GetEventTypesResponse como parte de sua solicitação. Um token de paginação nulo busca os registros desde o início	Lista	event-type		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetExternalModels	Concede permissão para obter os detalhes de um ou mais SageMaker modelos da Amazon que foram importados para o serviço. Esta é uma API paginada. Se você fornecer um maxResults nulo, essas ações recuperarão um máximo de 10 registros por página. Se você fornecer um maxResults, o valor deverá estar entre 5 e 10. Para obter os resultados da próxima página, forneça o token de paginação do GetExternalModelsResult como parte de sua solicitação. Um token de paginação nulo busca os registros desde o início	List	external-model		
GetKMSEncryptionKey	Concede permissão para obter a chave de criptografia se uma chave mestra do cliente (CMK) do Key Management Service (KMS) tiver sido especificada para criptografar conteúdo no Amazon Fraud Detector	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetLabels	Concede permissão para obter todos os rótulos ou um rótulo específico se o nome for fornecido. Esta é uma API paginada. Se você fornecer um maxResults nulo, essa ação recuperará um máximo de 50 registros por página. Se você fornecer um maxResults, o valor deverá estar entre 10 e 50. Para obter os resultados da próxima página, forneça o token de paginação do GetGetLabelsResponse como parte de sua solicitação. Um token de paginação nulo busca os registros desde o início	Lista	label		
GetListElements	Concede permissão para obter elementos de uma lista	Leitura	list*		
				aws:ResourceTag/${TagKey}	
GetListsMetadata	Concede permissão para obter metadados de uma lista	Lista	list		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetModelVersion	Concede permissão para obter os detalhes da versão do modelo especificada	Leitura	model-version*		
GetModels	Concede permissão para obter um ou mais modelos. Obtém todos os modelos Conta da AWS se nenhum tipo de modelo e nenhum ID de modelo for fornecido. Obtém todos os modelos para o tipo de modelo Conta da AWS e, se o tipo de modelo for especificado, mas o ID do modelo não for fornecido. Obtém um modelo específico se tupla (tipo de modelo, ID de modelo) for especificado	List	model		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetOutcomes	Concede permissão para obter um ou mais resultados. Esta é uma API paginada. Se você fornecer um maxResults nulo, essas ações recuperarão um máximo de 100 registros por página. Se você fornecer um maxResults, o valor deverá estar entre 50 e 100. Para obter os resultados da próxima página, forneça o token de paginação do GetOutcomesResult como parte de sua solicitação. Um token de paginação nulo busca os registros desde o início	List	outcome		
GetRules	Concede permissão para obter todas as regras para um detector (paginado) se ruleId e ruleVersion não estiverem especificados. Obterá todas as regras para o detector e o ruleId se houver (paginado). Obtém uma regra específica se tanto o ruleId como o ruleVersion forem especificados	List	rule		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetVariables	Concede permissão para obter todas as variáveis ou a variável específica. Esta é uma API paginada. Fornecer uma maxSizePer página nula resulta na recuperação máxima de 100 registros por página. Se você fornecer maxSizePer Página, o valor deverá estar entre 50 e 100. Para obter o resultado da próxima página, forneça um token de paginação GetVariablesResult como parte de sua solicitação. O token de paginação nulo busca os registros desde o início.	Lista	variable		
ListEventPredictions	Concede permissão para obter uma lista de previsões anteriores	Lista	detector		
			detector-version		
			event-type		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar todas as etiquetas associadas ao recurso. Esta é uma API paginada. Para obter os resultados da próxima página, forneça o token de paginação da resposta como parte da solicitação. Um token de paginação nulo busca os registros desde o início	Leitura	batch-import		
			batch-prediction		
			detector		
			detector-version		
			entity-type		
			event-type		
			external-model		
			label		
			list		
			model		
			model-version		
			outcome		
			rule		
			variable		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutDetector	Concede permissão para criar ou atualizar um detector	Write	detector*		
			event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutEntityType	Concede permissão para criar ou atualizar um tipo de entidade. Uma entidade representa quem está realizando o evento. Como parte de uma previsão de fraude, você transmite o ID da entidade para indicar a entidade específica que executou o evento. Um tipo de entidade classifica a entidade. Classificações de exemplo incluem cliente, comerciante ou conta	Write	entity-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutEventType	Concede permissão para criar ou atualizar um tipo de evento. Um evento é uma atividade comercial que é avaliada quanto ao risco de fraude. Com o Amazon Fraud Detector, você gera previsões de fraude para eventos. Um tipo de evento define a estrutura de um evento enviado ao Amazon Fraud Detector. Isso inclui as variáveis enviadas como parte do evento, a entidade que executa o evento (como um cliente) e os rótulos que classificam o evento. Os tipos de evento de exemplo incluem transações de pagamento online, registros de conta e autenticações	Gravar	event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutExternalModel	Concede permissão para criar ou atualizar um SageMaker modelo de endpoint da Amazon. Você também pode usar essa ação para atualizar a configuração do endpoint do modelo, incluindo a função and/or do IAM e as variáveis mapeadas.	Gravar	event-type*		
			external-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutKMSEncryptionKey	Concede permissão para especificar a chave mestra do cliente (CMK) do Key Management Service (KMS) a ser usada para criptografar conteúdo no Amazon Fraud Detector	Write			
PutLabel	Concede permissão para criar ou atualizar rótulos. Um rótulo classifica um evento como fraudulento ou legítimo. Os rótulos são associados a tipos de eventos e usados para treinar modelos supervisionados de machine learning no Amazon Fraud Detector.	Write	label*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutOutcome	Concede permissão para criar ou atualizar um resultado	Gravar	outcome*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
SendEvent	Concede permissão para enviar o evento	Gravar	event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Concede permissão para atribuir etiquetas a um recurso	Marcação	batch-import		
			batch-prediction		
			detector		
			detector-version		
			entity-type		
			event-type		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			external-model		
			label		
			list		
			model		
			model-version		
			outcome		
			rule		
			variable		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover etiquetas de um recurso	Marcação	batch-import		
			batch-prediction		
			detector		
			detector-version		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			entity-type		
			event-type		
			external-model		
			label		
			list		
			model		
			model-version		
			outcome		
			rule		
			variable		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateDetectorVersion	Concede permissão para atualizar uma versão de detector. Os atributos da versão do detector que você pode atualizar incluem modelos, endpoints de modelo externo, regras, modo de execução de regras e descrição. Você pode atualizar somente uma versão DRAFT do detector	Write	detector*		
			external-model		
			model-version		
UpdateDetectorVersionMetadata	Concede permissão para atualizar a descrição da versão do detector. Você pode atualizar os metadados de qualquer versão do detector (DRAFT, ACTIVE ou INACTIVE).	Gravar	detector-version*		
UpdateDetectorVersionStatus	Concede permissão para atualizar o status da versão do detector. Você pode realizar as seguintes promoções ou rebaixamentos usando UpdateDetectorVersionStatus : DRAFT para ATIVO, ATIVO para INATIVO e INATIVO para ATIVO	Gravar	detector-version*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateEventLabel	Concede permissão para atualizar o valor do rótulo de um registro de evento existente	Gravar	event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateList	Concede permissão para atualizar uma lista	Gravar	list*		
				aws:ResourceTag/${TagKey}	
UpdateModel	Concede permissão para atualizar um modelo É possível atualizar o atributo de descrição usando essa ação	Write	model*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateModelVersion	Concede permissão para atualizar uma versão do modelo. Atualizar uma versão de modelo treina novamente uma versão de modelo existente usando dados de treinamento atualizados e produz uma nova versão secundária do modelo. É possível atualizar o local do conjunto de dados de treinamento e os atributos de função de acesso a dados usando essa ação. Essa ação cria e treina uma nova versão secundária do modelo, por exemplo, a versão 1.01, 1.02, 1.03	Write	model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateModelVersionStatus	Concede permissão para atualizar o status de uma versão de modelo	Write	model-version*		
UpdateRuleMetadata	Concede permissão para atualizar os metadados de uma regra. O atributo de descrição pode ser atualizado	Write	rule*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateRuleVersion	Concede permissão para atualizar uma versão de regra, resultando em uma nova versão de regra. Atualiza uma versão de regra resultante para uma nova versão de regra (versão 1, 2, 3...)	Write	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateVariable	Concede permissão para atualizar uma variável	Write	variable*		

Tipos de recursos definidos pelo Amazon Fraud Detector

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
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}

Chaves de condição do Amazon Fraud Detector

O Amazon Fraud Detector define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra ações com base nas etiquetas transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra as ações com base nas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra ações com base nas chaves da etiqueta transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o nível gratuito da AWS

AWS O nível gratuito (prefixo do serviço:`freetier`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo nível gratuito da AWS
- Tipos de recursos definidos pelo nível gratuito da AWS
- Chaves de condição para o nível gratuito da AWS

Ações definidas pelo nível gratuito da AWS

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAccountActivity	Concede permissão para obter um registro de atividade específico	Leitura			
GetAccountPlanState	Concede permissão para obter todas as informações relacionadas ao estado do plano de conta relacionado ao nível gratuito	Leitura			
GetFreeTierAlertPreference	Concede permissão para obter a preferência de alerta	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
[somente permissão]	de nível gratuito (endereço de e-mail)				
GetFreeTierUsage	Concede permissão para obter limites de uso do nível gratuito e status de uso MTD	Leitura			
ListAccountActivities	Concede permissão para listar as atividades disponíveis	Lista			
PutFreeTierAlertPreference [somente permissão]	Concede permissão para definir a preferência de alerta de nível gratuito (endereço de e-mail)	Gravar			
UpgradeAccountPlan	Concede permissão para acionar uma atualização do plano da conta	Gravar			

Tipos de recursos definidos pelo nível gratuito da AWS

AWS O nível gratuito não suporta a especificação de um ARN de recurso no elemento de uma `Resource` declaração de política do IAM. Para conceder acesso ao nível gratuito da AWS , especifique `"Resource": "*"` na política.

Chaves de condição para o nível gratuito da AWS

O nível gratuito não tem chaves de contexto específicas ao serviço que possam ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do Amazon FreeRTOS

O Amazon FreeRTOS (prefixo do serviço: `freertos`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon FreeRTOS
- Tipo de recursos definidos pelo Amazon FreeRTOS
- Chaves de condição do Amazon FreeRTOS

Ações definidas pelo Amazon FreeRTOS

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSoftwareConfiguration	Concede permissão para criar uma configuração de software	Gravar	configuration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscription	Concede permissão para criar uma assinatura do plano de manutenção estendida (EMP) FreeRTOS	Gravar		aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
DeleteSoftwareConfiguration	Concede permissão para excluir a configuração de software	Gravar	configuration*		
DescribeHardwarePlatform	Concede permissão para descrever a plataforma de hardware	Leitura			
DescribeSoftwareConfiguration	Concede permissão para descrever a configuração de software	Leitura	configuration*		
DescribeSubscription	Concede permissão para descrever a assinatura para o plano de manutenção estendida (EMP) FreeRTOS	Leitura	subscription*		
GetEmpPatchUrl	Concede permissão para obter URL de versões de patches, diferenças de patches e notas da versão de software no plano de manutenção estendida (EMP) FreeRTOS	Leitura			
GetSoftwareURL	Concede permissão para obter o URL para baixar o software do Amazon FreeRTOS	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSoftwareURLForConfiguration	Concede permissão para obter o URL para baixar o software do Amazon FreeRTOS com base na configuração	Leitura			
GetSubscriptionBillingAmount	Concede permissão para buscar o valor de faturamento da assinatura para o plano de manutenção estendida (EMP) FreeRTOS	Leitura			
ListFreeRTOSVersions	Concede permissão para listas de versões do AmazonFree RTOS	Lista			
ListHardwarePlatforms	Concede permissão para listar plataformas de hardware	Lista			
ListHardwareVendors	Concede permissão para listar fornecedores de hardware	Lista			
ListSoftwareConfigurations	Concede permissão para listar as configurações de software	Lista			
ListSoftwarePatches	Concede permissão para listar patches de software de uma assinatura para o plano de manutenção estendida (EMP) FreeRTOS	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListSubscriptionEmails	Concede permissão para listar e-mails de assinatura para o plano de manutenção estendida (EMP) FreeRTOS	Lista			
ListSubscriptions	Concede permissão para listar as assinaturas para o plano de manutenção estendida (EMP) FreeRTOS	Lista			
UpdateEmailRecipients	Concede permissão para atualizar a lista de endereços de e-mail de assinatura do plano de manutenção estendida (EMP) FreeRTOS	Gravar			
UpdateSoftwareConfiguration	Concede permissão para atualizar a configuração de software	Gravar	configuration*		
VerifyEmail	Concede permissão para verificar o e-mail para o plano de manutenção estendida (EMP) FreeRTOS	Gravar			

Tipo de recursos definidos pelo Amazon FreeRTOS

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves

são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
configuration	`arn:${Partition}:freertos:${Region}:${Account}:configuration/${ConfigurationName}`	aws:ResourceTag/${TagKey}
subscription	`arn:${Partition}:freertos:${Region}:${Account}:subscription/${SubscriptionID}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon FreeRTOS

O Amazon FreeRTOS define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por chave de tag presente na solicitação que o usuário faz ao Amazon FreeRTOS	String
aws:ResourceTag/${TagKey}	Filtra o acesso por componente de chave de tag anexado a um recurso do Amazon FreeRTOS	String
aws:TagKeys	Filtra o acesso pela lista de todos os nomes de chave da etiqueta associados ao recurso na solicitação	ArrayOfString

Ações, recursos e chaves de condição para a Amazon FSx

A Amazon FSx (prefixo do serviço:`fsx`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon FSx
- Tipos de recursos definidos pela Amazon FSx
- Chaves de condição para a Amazon FSx

Ações definidas pela Amazon FSx

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateFileGateway [somente permissão]	Concede permissão para associar uma instância do File Gateway a um sistema de arquivos Amazon FSx para Windows File Server	Gravar	file-system*		
AssociateFileSystemAliases	Concede permissão para associar aliases de DNS a um sistema de arquivos Amazon FSx para Windows File Server	Gravar	file-system*		
BypassSnaplockEnte	Concede permissão para permitir a exclusão de um	Gerenciamento de	volume*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
rpriseRetention [somente permissão]	FSx volume do ONTAP SnapLock Enterprise que contém arquivos WORM (grave uma vez, leia vários) com períodos de retenção ativos	permissões			
CancelDataRepositoryTask	Concede permissão para cancelar uma tarefa de repositório de dados	Gravação	task*		
CopyBackup	Concede permissão para copiar um backup	Gravar	backup*		fsx:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CopySnapshotAndUpdateVolume	Concede permissão para atualizar um volume existente usando um snapshot de outro sistema de arquivos Amazon FSx for OpenZFS	Gravar	snapshot*		
			volume*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAndAttachS3AccessPoint	Concede permissão para criar e anexar um ponto de acesso S3 a um sistema de FSx arquivos	Gravar	volume		s3:CreateAccessPoint s3:GetAccessPoint s3:PutAccessPointPolicy
CreateBackup	Concede permissão para criar um novo backup de um sistema de FSx arquivos da Amazon ou de um FSx volume da Amazon	Gravar	backup*		fsx:TagResource
			file-system		
			volume		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataRepositoryAssociation	Concede permissão para criar uma nova associação de repositório de dados para um sistema de arquivos Amazon FSx for Lustre	Gravar	association*		fsx:TagResource
			file-system*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataRepositoryTask	Concede permissão para criar uma nova tarefa de repositório de dados para um sistema de arquivos Amazon FSx for Lustre	Gravar	file-system*		fsx:TagResource
			task*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateFileCache	Concede permissão para criar um novo cache de arquivos Amazon vazio	Gravar	file-cache*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:GetSecurityGroupsForVpc fsx:CreateDataRepositoryAssociation fsx:TagResource logs:CreateLogGroup logs:CreateLogStream logs:PutLogEvents

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					s3:ListBucket
			association	fsx:NfsDataRepositoryEncryptionInTransitEnabled fsx:NfsDataRepositoryAuthenticationEnabled	
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFileSystem	Concede permissão para criar um novo sistema de FSx arquivos da Amazon vazio	Gravar	file-system*		ec2:GetSecurityGroupsForVpc fsx:TagResource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFileSystemFromBackup	Concede permissão para criar um novo sistema de FSx arquivos da Amazon a partir de um backup existente	Gravar	backup*		ec2:GetSecurityGroupsForVpc fsx:TagResource
			file-system*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshot	Concede permissão para criar um novo snapshot em um volume	Gravar	snapshot*		fsx:TagResource
			volume*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStorageVirtualMachine	Concede permissão para criar uma nova máquina virtual de armazenamento em um sistema de arquivos Amazon FSx for Ontap	Gravar	file-system*		fsx:TagResource
			storage-virtual-machine*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVolume	Concede permissão para criar um novo volume	Gravar	volume*		fsx:TagResource
			snapshot		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys fsx:StorageVirtualMachineId fsx:ParentVolumeId	
CreateVolumeFromBackup	Concede permissão para criar um novo volume a partir do backup	Gravar	backup*		fsx:TagResource
			storage-virtual-machine*		
			volume*		
				aws:RequestTag/${TagKey} aws:TagKeys fsx:StorageVirtualMachineId	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteBackup	Concede permissão para excluir um backup, excluindo seu conteúdo. Após a exclusão, o backup não existe mais e seus dados não estão mais disponíveis	Gravar	backup*		
DeleteDataRepositoryAssociation	Concede permissão para excluir uma associação de repositório de dados	Gravar	association*		
DeleteFileCache	Concede permissão para excluir um cache de arquivos, excluindo seu conteúdo	Gravar	file-cache*		fsx:DeleteDataRepositoryAssociation
			association		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFileSystem	Concede permissão para excluir um sistema de arquivos, excluindo seu conteúdo e quaisquer backups automáticos existentes do sistema de arquivos	Gravar	file-system*		fsx:CreateBackup fsx:TagResource
			backup		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteResourcePolicy [somente permissão]	Necessário para gerenciar o compartilhamento de FSx volumes entre contas por meio do AWS Resource Access Manager (RAM). PutResourcePolicy e também GetResourcePolicy são obrigatórios	Gerenciamento de permissões	volume*		
DeleteSnapshot	Concede permissão para excluir um snapshot em um volume	Gravar	snapshot*		
DeleteStorageVirtualMachine	Concede permissão para excluir uma máquina virtual de armazenamento, excluindo seu conteúdo	Gravar	storage-virtual-machine*		
DeleteVolume	Concede permissão para excluir um volume, excluindo seu conteúdo e quaisquer backups automáticos existentes do volume	Gravar	volume*		fsx:TagResource
			backup		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys fsx:StorageVirtualMachineId fsx:ParentVolumeId	
DescribeAssociatedFileGateways [somente permissão]	Concede permissão para descrever as instâncias do File Gateway associadas a um sistema de arquivos Amazon FSx para Windows File Server	Leitura	file-system*		
DescribeBackups	Concede permissão para retornar as descrições de todos os backups Região da AWS de sua propriedade Conta da AWS no endpoint que você está chamando	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeDataRepositoryAssociations	Concede permissão para retornar as descrições de todas as associações de repositórios de dados pertencentes a Região da AWS você Conta da AWS no endpoint que você está chamando	Leitura			
DescribeDataRepositoryTasks	Concede permissão para retornar as descrições de todas as tarefas do repositório de dados Região da AWS de sua propriedade Conta da AWS no endpoint que você está chamando	Leitura			
DescribeFileCaches	Concede permissão para retornar as descrições de todos os caches de arquivos Região da AWS de sua propriedade Conta da AWS no endpoint que você está chamando	Leitura			
DescribeFileSystemAliases	Concede permissão para retornar a descrição de todos os aliases de DNS pertencentes ao seu sistema de arquivos Amazon FSx para Windows File Server	Leitura	file-system*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeFileSystems	Concede permissão para retornar as descrições de todos os sistemas de arquivos Região da AWS de sua propriedade Conta da AWS no endpoint que você está chamando	Leitura			
DescribeS3AccessPointAttachments	Concede permissão para retornar as descrições dos anexos do ponto de acesso S3	Leitura			
DescribeSharedVpcConfiguration	Concede permissão para retornar as descrições sobre se as atualizações da tabela de FSx rotas das contas dos participantes são permitidas em sua conta	Leitura			
DescribeSnapshots	Concede permissão para retornar as descrições de todos os instantâneos Região da AWS de sua propriedade Conta da AWS no endpoint que você está chamando	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeStorageVirtualMachines	Concede permissão para retornar as descrições de todas as máquinas virtuais de armazenamento Região da AWS de sua propriedade Conta da AWS no endpoint que você está chamando	Leitura			
DescribeVolumes	Concede permissão para retornar as descrições de todos os volumes Região da AWS de sua propriedade Conta da AWS no endpoint que você está chamando	Leitura			
DetachAndDeleteS3AccessPoint	Concede permissão para separar um ponto de acesso S3 de um sistema de FSx arquivos da Amazon e excluir o ponto de acesso S3	Gravar	volume		s3:DeleteAccessPoint
DisassociateFileGateway [somente permissão]	Concede permissão para desassociar uma instância do File Gateway de um sistema de arquivos Amazon FSx para Windows File Server	Gravar	file-system*		
DisassociateFileSystemAliases	Concede permissão para dissociar aliases do sistema de arquivos de um sistema de arquivos Amazon FSx para Windows File Server	Gravar	file-system*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetResourcePolicy [somente permissão]	Necessário para gerenciar o compartilhamento de FSx volumes entre contas por meio do AWS Resource Access Manager (RAM). PutResourcePolicy e também DeleteResourcePolicy são obrigatórios	Gerenciamento de permissões	volume*		
ListTagsForResource	Concede permissão para listar tags para um FSx recurso da Amazon	Leitura	association		
			backup		
			file-cache		
			file-system		
			snapshot		
			storage-virtual-machine		
			task		
			volume		
ManageBackupPrincipalAssociations [somente permissão]	Concede permissão para gerenciar associações principais de backup por meio do AWS Backup	Gerenciamento de permissões	backup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutResourcePolicy [somente permissão]	Necessário para gerenciar o compartilhamento de FSx volumes entre contas por meio do AWS Resource Access Manager (RAM). DeleteResourcePolicy e também GetResourcePolicy são obrigatórios	Gerenciamento de permissões	volume*		
ReleaseFileSystemNfsV3Locks	Concede permissão para liberar bloqueios do sistema de arquivos NFS V3	Gravar	file-system*		
RestoreVolumeFromSnapshot	Concede permissão para restaurar o estado do volume de um snapshot	Gravar	snapshot*		
			volume*		
StartMisconfiguredStateRecovery	Concede permissão para iniciar a recuperação de estado configurado incorretamente	Gravar	file-system*		
TagResource	Concede permissão para marcar um FSx recurso da Amazon	Tags	association		
			backup		
			file-cache		
			file-system		
			snapshot		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			storage-virtual-machine		
			task		
			volume		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover uma tag de um FSx recurso da Amazon	Tags	association		
			backup		
			file-cache		
			file-system		
			snapshot		
			storage-virtual-machine		
			task		
			volume		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
UpdateDataRepositoryAssociation	Concede permissão para atualizar a configuração de associação de repositório	Gravar	association*		
UpdateFileCache	Concede permissão para atualizar a configuração do cache de arquivos	Gravar	file-cache*		
UpdateFileSystem	Concede permissão para atualizar a configuração do sistema de arquivos	Gravar	file-system*		
UpdateSharedVpcConfiguration	Concede permissão para ativar ou desativar as atualizações da tabela de FSx rotas das contas dos participantes em sua conta	Gravar			
UpdateSnapshot	Concede permissão para atualizar uma configuração de snapshot	Gravar	snapshot*		
UpdateStorageVirtualMachine	Concede permissão para atualizar uma configuração de máquina virtual de armazenamento	Gravar	storage-virtual-machine*		
UpdateVolume	Concede permissão para atualizar uma configuração de volume	Gravar	volume*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				fsx:StorageVirtualMachineId fsx:ParentVolumeId	

Tipos de recursos definidos pela Amazon FSx

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

> **Note**
>
> Amazon FSx para Windows File Server, Lustre e Ontap compartilham alguns dos mesmos tipos de recursos, com o mesmo formato ARN para cada um.

Tipos de recursos	ARN	Chaves de condição
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}

Tipos de recursos	ARN	Chaves de condição
backup	`arn:${Partition}:fsx:${Region}:${Account}:backup/${BackupId}`	aws:ResourceTag/${TagKey}
storage-virtual-machine	`arn:${Partition}:fsx:${Region}:${Account}:storage-virtual-machine/${FileSystemId}/${StorageVirtualMachineId}`	aws:ResourceTag/${TagKey}
task	`arn:${Partition}:fsx:${Region}:${Account}:task/${TaskId}`	aws:ResourceTag/${TagKey}
association	`arn:${Partition}:fsx:${Region}:${Account}:association/${FileSystemIdOrFileCacheId}/${DataRepositoryAssociationId}`	aws:ResourceTag/${TagKey}
volume	`arn:${Partition}:fsx:${Region}:${Account}:volume/${FileSystemId}/${VolumeId}`	aws:ResourceTag/${TagKey}
snapshot	`arn:${Partition}:fsx:${Region}:${Account}:snapshot/${VolumeId}/${SnapshotId}`	aws:ResourceTag/${TagKey}

Chaves de condição para a Amazon FSx

A Amazon FSx define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString
fsx:IsBackupCopyDestination	Filtra o acesso pelo fato de o backup ser um backup de destino para uma CopyBackup operação	Bool
fsx:IsBackupCopySource	Filtra o acesso pelo fato de o backup ser um backup de origem para uma CopyBackup operação	Bool
fsx:NfsDataRepositoryAuthenticationEnabled	Filtra o acesso por repositórios de dados NFS que oferecem suporte à autenticação	Bool
fsx:NfsDataRepositoryEncryptionInTransitEnabled	Filtra o acesso por repositórios de dados NFS que suportam encryption-in-transit	Bool
fsx:ParentVolumeId	Filtra o acesso pela volume pai que contém para operações de volume mutantes	String
fsx:StorageVirtualMachineId	Filtra o acesso pela máquina virtual de armazenamento que contém um volume para operações de volume mutantes	String

Ações, recursos e chaves de condição para GameLift servidores Amazon

A Amazon GameLift Servers (prefixo do serviço:`gamelift`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelos GameLift servidores da Amazon
- Tipos de recursos definidos pelos GameLift servidores da Amazon
- Chaves de condição para GameLift servidores Amazon

Ações definidas pelos GameLift servidores da Amazon

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptMatch	Concede permissão para registrar a aceitação ou rejeição de um jogador em uma FlexMatch partida proposta	Gravar			
ClaimGameServer	Concede permissão para localizar e reservar um servidor de jogos para hospedar uma nova sessão de jogo	Write	gameServerGroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAlias	Concede permissão para definir um novo alias para uma frota	Write		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreateBuild	Concede permissão para criar uma nova compilação de jogo usando arquivos armazenados em um bucket do Amazon S3	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource iam:PassRole s3:GetObject
CreateContainerFleet	Concede permissão para criar uma nova frota de contêineres de recursos de computação para executar seus servidores de jogos	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeAvailabilityZones ec2:DescribeRegions gamelift:TagResource iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateContainerGroupDefinition	Concede permissão para criar uma nova definição de grupo de contêineres usando imagens armazenadas em um repositório Amazon ECR	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	ecr:BatchGetImage ecr:DescribeImages ecr:GetAuthorizationToken ecr:GetDownloadUrlForLayer gamelift:TagResource
CreateFleet	Concede permissão para criar uma nova frota de recursos de computação para executar seus servidores de jogos	Write		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeAvailabilityZones ec2:DescribeRegions gamelift:TagResource iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateFleetLocations	Concede permissão para especificar locais adicionais para uma frota	Write	containerFleet		ec2:DescribeAvailabilityZones ec2:DescribeRegions
			fleet		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateGameServerGroup	Concede permissão para criar um novo grupo de servidores de jogos, configurar um grupo de Auto Scaling correspondente e iniciar instâncias para hospedar servidores de jogos	Write		aws:RequestTag/${TagKey} aws:TagKeys	autoscaling:CreateAutoScalingGroup autoscaling:DescribeAutoScalingGroups autoscaling:PutLifecycleHook autoscaling:PutScalingPolicy ec2:DescribeAvailabilityZones ec2:DescribeSubnets events:PutRule events:PutTargets

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					gamelift:TagResource iam:PassRole
CreateGameSession	Concede permissão para iniciar uma nova sessão de jogo em uma frota especificada	Write			
CreateGameSessionQueue	Concede permissão para configurar uma nova fila para processar solicitações de colocação de sessão de jogo	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreateLocation	Concede permissão para definir um novo local para uma frota	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreateMatchmakingConfiguration	Concede permissão para criar um novo FlexMatch matchmaker	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateMatchmakingRuleSet	Concede permissão para criar um novo conjunto de regras de matchmaking para FlexMatch	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreatePlayerSession	Concede permissão para reservar um slot de sessão de jogo disponível para um jogador	Write			
CreatePlayerSessions	Concede permissão para reservar slots de sessão de jogo disponíveis para vários jogadores	Write			
CreateScript	Concede permissão para criar um novo script de servidores em tempo real	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource iam:PassRole s3:GetObject

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateVpcPeeringAuthorization	Concede permissão para permitir GameLift a criação ou exclusão de uma conexão de emparelhamento entre uma VPC de GameLift frota e uma VPC em outra Conta da AWS	Gravar			ec2:AcceptVpcPeeringConnection ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateRoute ec2:DeleteRoute ec2:DescribeRouteTables ec2:DescribeSecurityGroups ec2:RevokeSecurityGroupEgress

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:RevokeSecurityGroupIngress
CreateVpcPeeringConnection	Concede permissão para estabelecer uma conexão de emparelhamento entre a VPC GameLift da sua frota e uma VPC em outra conta	Gravar			
DeleteAlias	Concede permissão para excluir um alias	Write	alias*		
DeleteBuild	Concede permissão para excluir uma compilação de jogo	Gravar	build*		
DeleteContainerFleet	Concede permissão para excluir uma frota de contêineres	Gravar	containerFleet*		
DeleteContainerGroupDefinition	Concede permissão para excluir uma definição de grupo de contêineres	Gravar	containerGroupDefinition*		
DeleteFleet	Concede permissão para excluir uma frota vazia	Write	fleet*		
DeleteFleetLocations	Concede permissão para excluir locais de uma frota	Write	containerFleet		
			fleet		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteGameServerGroup	Concede permissão para excluir permanentemente um grupo de servidores de jogos e encerrar a atividade do FleeTiq para o grupo de Auto Scaling correspondente	Write	gameServerGroup*		autoscaling:DeleteAutoScalingGroup autoscaling:DescribeAutoScalingGroups autoscaling:ExitStandby autoscaling:ResumeProcesses autoscaling:SetInstanceProtection autoscaling:UpdateAutoScalingGroup
DeleteGameSessionQueue	Concede permissão para excluir uma fila de sessão de jogo existente	Gravar	gameSessionQueue*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteLocation	Concede permissão para excluir um local.	Gravar	location*		
DeleteMatchmakingConfiguration	Concede permissão para excluir um FlexMatch matchmaker existente	Gravar	matchmakingConfiguration*		
DeleteMatchmakingRuleSet	Concede permissão para excluir um conjunto de regras de FlexMatch matchmaking existente	Gravar	matchmakingRuleSet*		
DeleteScalingPolicy	Concede permissão para excluir um conjunto de regras de autoescalabilidade	Write	containerFleet		
			fleet		
DeleteScript	Concede permissão para excluir um script de servidores em tempo real	Write	script*		
DeleteVpcPeeringAuthorization	Concede permissão para cancelar uma autorização de emparelhamento de VPC	Gravar			
DeleteVpcPeeringConnection	Concede permissão para remover uma conexão de emparelhamento entre VPCs	Gravar			
DeregisterCompute	Concede permissão para cancelar o registro de um computador para uma frota	Gravar	fleet*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeregisterGameServer	Concede permissão para remover um servidor de jogos de um grupo de servidores de jogos	Write	gameServerGroup*		
DescribeAlias	Concede permissão para recuperar propriedades de um alias	Read	alias*		
DescribeBuild	Concede permissão para recuperar propriedades de uma compilação de jogo	Leitura	build*		
DescribeCompute	Concede permissão para recuperar informações para um computador em uma frota	Leitura	containerFleet		
			fleet		
DescribeContainerFleet	Concede permissão para recuperar as propriedades de uma frota de contêineres existente	Leitura	containerFleet*		
DescribeContainerGroupDefinition	Concede permissão para recuperar as propriedades de uma definição de grupo de contêineres existente	Leitura	containerGroupDefinition*		
DescribeEC2InstanceLimits	Concede permissão para recuperar o uso máximo permitido e atual para os tipos de EC2 instância	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeFleetAttributes	Concede permissão para recuperar propriedades gerais, incluindo status, para frotas	Leitura			
DescribeFleetCapacity	Concede permissão para recuperar as configurações de capacidade atuais para frotas gerenciadas	Leitura			
DescribeFleetDeployment	Concede permissão para recuperar as propriedades de uma implantação de frota existente	Leitura	containerFleet*		
DescribeFleetEvents	Concede permissão para recuperar entradas do log de eventos de uma frota	Read	containerFleet		
			fleet		
DescribeFleetLocationAttributes	Concede permissão para recuperar propriedades gerais, incluindo status, para locais de uma frota	Read	containerFleet		
			fleet		
DescribeFleetLocationCapacity	Concede permissão para recuperar a configuração de capacidade atual para a localização de uma frota	Read	containerFleet		
			fleet		
DescribeFleetLocationUtilization	Concede permissão para recuperar estatísticas de utilização para a localização da frota	Read	fleet*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeFleetPortSettings	Concede permissão para recuperar as permissões de conexão de entrada para uma frota	Read	fleet*		
DescribeFleetUtilization	Concede permissão para recuperar estatísticas de utilização para frotas	Read			
DescribeGameServer	Concede permissão para recuperar propriedades de um servidor de jogo	Read	gameServerGroup*		
DescribeGameServerGroup	Concede permissão para recuperar propriedades de um grupo de servidores de jogos	Leitura	gameServerGroup*		
DescribeGameServerInstances	Concede permissão para recuperar o status das EC2 instâncias em um grupo de servidores de jogos	Leitura	gameServerGroup*		
DescribeGameSessionDetails	Concede permissão para recuperar propriedades para sessões de jogo em uma frota, incluindo a política de proteção	Read			
DescribeGameSessionPlacement	Concede permissão para recuperar detalhes de uma solicitação de colocação de sessão de jogo	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeGameSessionQueues	Concede permissão para recuperar propriedades para filas de sessões de jogo	Read			
DescribeGameSessions	Concede permissão para recuperar propriedades de sessões de jogo em uma frota	Leitura			
DescribeInstances	Concede permissão para recuperar informações sobre instâncias em uma frota gerenciada	Leitura	containerFleet		
			fleet		
DescribeMatchmaking	Concede permissão para recuperar detalhes de tickets de marcação de jogos	Leitura			
DescribeMatchmakingConfigurations	Concede permissão para recuperar propriedades para matchmakers FlexMatch	Leitura			
DescribeMatchmakingRuleSets	Concede permissão para recuperar propriedades para conjuntos de regras de FlexMatch matchmaking	Leitura			
DescribePlayerSessions	Concede permissão para recuperar propriedades de sessões de jogadores em uma sessão de jogo	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeRuntimeConfiguration	Concede permissão para recuperar a configuração de runtime atual de uma frota	Read	fleet*		
DescribeScalingPolicies	Concede permissão para recuperar todas as políticas de dimensionamento aplicadas a uma frota	Read	containerFleet		
			fleet		
DescribeScript	Concede permissão para recuperar propriedades de um script de servidores em tempo real	Read	script*		
DescribeVpcPeeringAuthorizations	Concede permissão para recuperar autorizações válidas de emparelhamento de VPC	Read			
DescribeVpcPeeringConnections	Concede permissão para recuperar detalhes sobre conexões de emparelhamento VPC ativas ou pendentes	Leitura			
GetComputeAccess	Concede permissão para recuperar credenciais para acessar remotamente uma computação em uma frota gerenciada	Leitura	containerFleet		
			fleet		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetComputeAuthToken	Concede permissão para recuperar um token de autenticação que permite que processos em um computador enviem solicitações para o serviço da Amazon GameLift	Leitura	containerFleet		
			fleet		
GetGameSessionLogUrl	Concede permissão para recuperar o local dos logs armazenados para uma sessão de jogo	Read			
GetInstanceAccess	Concede permissão para solicitar acesso remoto a uma instância de frota especificada	Read	fleet*		
ListAliases	Concede permissão para recuperar todos os aliases definidos na região atual	List			
ListBuilds	Concede permissão para recuperar toda a compilação do jogo na região atual	Lista			
ListCompute	Concede permissão para recuperar todos os recursos de computação na região atual	Lista	containerFleet		
			fleet		
ListContainerFleets	Concede permissão para recuperar as propriedades de todas as frotas de contêineres existentes na região atual	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListContainerGroupDefinitionVersions	Concede permissão para recuperar as propriedades de todas as versões de uma definição de grupo de contêineres existente	Lista	containerGroupDefinition*		
ListContainerGroupDefinitions	Concede permissão para recuperar as propriedades de todas as definições de grupos de contêineres existentes na região atual	Lista			
ListFleetDeployments	Concede permissão para recuperar as propriedades de todas as implantações de frota existentes na região atual	Lista			
ListFleets	Concede permissão para recuperar uma lista de frotas IDs para todas as frotas na região atual	Lista			
ListGameServerGroups	Concede permissão para recuperar todos os grupos de servidores de jogos definidos na região atual	List			
ListGameServers	Concede permissão para recuperar todos os servidores de jogos que estão sendo executados no momento em um grupo de servidores de jogos	Lista	gameServerGroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListLocations	Concede permissão para recuperar todos os locais desta conta	Lista			
ListScripts	Concede permissão para recuperar propriedades para todos os scripts de servidores em tempo real na região atual	Lista			
ListTagsForResource	Concede permissão para recuperar tags para recursos GameLift	Leitura	alias		
			build		
			containerFleet		
			containerGroupDefinition		
			fleet		
			gameServerGroup		
			gameSessionQueue		
			location		
			matchmakingConfiguration		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			matchmakingRuleSet		
			script		
PutScalingPolicy	Concede permissão para criar ou atualizar uma política de autoescalabilidade de frota	Gravar	containerFleet		
			fleet		
RegisterCompute	Concede permissão para registrar um computador para uma frota	Gravar	fleet*		
RegisterGameServer	Concede permissão para notificar o GameLift FleetiQ quando um novo servidor de jogos estiver pronto para hospedar o jogo	Gravar	gameServerGroup*		
RequestUploadCredentials	Concede permissão para recuperar novas credenciais de upload para usar ao fazer upload de uma nova compilação de jogo	Read	build*		
ResolveAlias	Concede permissão para recuperar o ID da frota associado a um alias	Read	alias*		
ResumeGameServerGroup	Concede permissão para restabelecer a atividade suspensa do FleeTIQ para um grupo de servidores de jogos	Write	gameServerGroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SearchGameSessions	Concede permissão para recuperar sessões de jogo que correspondam a um conjunto de critérios de pesquisa	Leitura			
StartFleetActions	Concede permissão para retomar a atividade de auto-scaling em uma frota depois que ela foi suspensa com () StopFleetActions	Gravar	containerFleet		
			fleet		
StartGameSessionPlacement	Concede permissão para enviar uma solicitação de colocação de sessão de jogo para uma fila de sessão de jogo	Gravar	gameSessionQueue*		
StartMatchBackfill	Concede permissão para solicitar FlexMatch matchmaking para preencher as vagas disponíveis para jogadores em uma sessão de jogo existente	Gravar			
StartMatchmaking	Concede permissão para solicitar FlexMatch matchmaking para um ou um grupo de jogadores e iniciar a colocação da sessão de jogo	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopFleetActions	Concede permissão para suspender a atividade de autoescalabilidade em uma frota	Write	containerFleet		
			fleet		
StopGameSessionPlacement	Concede permissão para cancelar uma solicitação de colocação de sessão de jogo em andamento	Write			
StopMatchmaking	Concede permissão para cancelar uma solicitação de marcação de jogos ou de alocação de correspondência em andamento	Write			
SuspendGameServerGroup	Concede permissão para interromper temporariamente a atividade do FleeTIQ de um grupo de servidores de jogos	Gravar	gameServerGroup*		
TagResource	Concede permissão para marcar GameLift recursos	Tags	alias		
			build		
			containerFleet		
			containerGroupDefinition		
			fleet		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			gameServerGroup		
			gameSessionQueue		
			location		
			matchmakingConfiguration		
			matchmakingRuleSet		
			script		
				aws:RequestTag/${TagKey} aws:TagKeys	
Terminate GameSession	Concede permissão para encerrar uma sessão de jogo existente	Gravar			
UntagResource	Concede permissão para desmarcar recursos GameLift	Tags	alias		
			build		
			containerFleet		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			containerGroupDefinition		
			fleet		
			gameServerGroup		
			gameSessionQueue		
			location		
			matchmakingConfiguration		
			matchmakingRuleSet		
			script		
				aws:TagKeys	
UpdateAlias	Concede permissão para atualizar as propriedades de um alias existente	Write	alias*		
UpdateBuild	Concede permissão para atualizar os metadados de uma compilação existente	Gravar	build*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateContainerFleet	Concede permissão para atualizar uma frota de contêineres existente	Gravar	containerFleet*		
UpdateContainerGroupDefinition	Concede permissão para atualizar as propriedades de uma definição de grupo de contêineres existente	Gravar	containerGroupDefinition*		ecr:BatchGetImage ecr:DescribeImages ecr:GetAuthorizationToken ecr:GetDownloadUrlForLayer
UpdateFleetAttributes	Concede permissão para atualizar as propriedades gerais de uma frota existente	Gravar	fleet*		
UpdateFleetCapacity	Concede permissão para ajustar as configurações de capacidade de uma frota gerenciada	Gravar	containerFleet fleet		
UpdateFleetPortSettings	Concede permissão para ajustar as configurações de porta de uma frota	Write	fleet*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateGameServer	Concede permissão para alterar propriedades do servidor de jogo, status de integridade ou status de utilização	Write	gameServerGroup*		
UpdateGameServerGroup	Concede permissão para atualizar propriedades de grupo de servidores de jogos, incluindo tipos de instância permitidos	Write	gameServerGroup*		iam:PassRole
UpdateGameSession	Concede permissão para atualizar as propriedades de uma sessão de jogo existente	Write			
UpdateGameSessionQueue	Concede permissão para atualizar propriedades de uma fila de sessão de jogo existente	Gravar	gameSessionQueue*		
UpdateMatchmakingConfiguration	Concede permissão para atualizar as propriedades de uma configuração de FlexMatch matchmaking existente	Gravar	matchmakingConfiguration*		
UpdateRuntimeConfiguration	Concede permissão para atualizar como os processos do servidor são configurados em instâncias em uma frota existente	Write	fleet*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateScript	Concede permissão para atualizar os metadados e o conteúdo de um script existente de servidores Realtime	Gravar	script*		iam:PassRole s3:GetObject
ValidateMatchmakingRuleSet	Concede permissão para validar a sintaxe de um conjunto de regras de FlexMatch matchmaking	Leitura			

Tipos de recursos definidos pelos GameLift servidores da Amazon

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Tipos de recursos	ARN	Chaves de condição
containerFleet	arn:${Partition}:gamelift:${Region}:${Account}:containerfleet/${FleetId}	aws:ResourceTag/${TagKey}
fleet	arn:${Partition}:gamelift:${Region}:${Account}:fleet/${FleetId}	aws:ResourceTag/${TagKey}
gameServerGroup	arn:${Partition}:gamelift:${Region}:${Account}:gameservergroup/${GameServerGroupName}	aws:ResourceTag/${TagKey}
gameSessionQueue	arn:${Partition}:gamelift:${Region}:${Account}:gamesessionqueue/${GameSessionQueueName}	aws:ResourceTag/${TagKey}
location	arn:${Partition}:gamelift:${Region}:${Account}:location/${LocationId}	aws:ResourceTag/${TagKey}
matchmakingConfiguration	arn:${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}

Chaves de condição para GameLift servidores Amazon

A Amazon GameLift Servers define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o Amazon GameLift Streams

O Amazon GameLift Streams (prefixo do serviço:`gameliftstreams`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon GameLift Streams
- Tipos de recursos definidos pelo Amazon GameLift Streams
- Chaves de condição para Amazon GameLift Streams

Ações definidas pelo Amazon GameLift Streams

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddStreamGroupLocations	Concede permissão para anexar um local StreamGroup remoto	Gravar	streamgroup*		ec2:DescribeRegions
AssociateApplications	Concede permissão para associar aplicativos a um StreamGroup	Gravar	application*		
			streamgroup*		
CreateApplication	Concede permissão para criar aplicação	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	gameliftstreams:TagResource s3:GetObject s3:ListBucket
CreateStreamGroup	Concede permissão para criar um StreamGroup	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	gameliftstreams:TagResource
CreateStreamSessionConnection	Concede permissão para criar uma conexão de sessão de stream	Gravar	streamgroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteApplication	Concede permissão para excluir um aplicativo	Gravar	application*		
DeleteStreamGroup	Concede permissão para excluir um StreamGroup	Gravar	streamgroup*		
DisassociateApplications	Concede permissão para desassociar aplicativos de um StreamGroup	Gravar	application*		
			streamgroup*		
ExportStreamSessionFiles	Concede permissão para exportar arquivos de sessão de stream que seu aplicativo gera	Gravar	streamgroup*		s3:PutObject
GetApplication	Concede permissão para obter uma aplicação	Leitura	application*		
GetStreamGroup	Concede `permissão` para obter um StreamGroup	Leitura	streamgroup*		
GetStreamSession	Concede permissão para obter uma sessão de transmissão	Leitura	streamgroup*		
ListApplications	Concede permissão para listar aplicações	Lista			
ListStreamGroups	Concede permissão para listar StreamGroups	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListStreamSessions	Concede permissão para listar sessões de stream	Leitura	stream group*		
ListStreamSessionsByAccount	Concede permissão para listar sessões de stream	Leitura			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	application		
			stream group		
RemoveStreamGroupLocations	Concede permissão para separar um local StreamGroup remoto	Gravar	stream group*		
StartStreamSession	Concede permissão para criar uma sessão de transmissão	Gravar	stream group*		
TagResource	Concede permissão para marcar um recurso	Tags	application		
			stream group		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TerminateStreamSession	Concede permissão para encerrar uma sessão de transmissão	Gravar	streamgroup*		
UntagResource	Concede permissão para desmarcar um recurso	Marcação	application		
			streamgroup		
				aws:TagKeys	
UpdateApplication	Concede permissão para atualizar uma aplicação	Gravar	application*		
UpdateStreamGroup	Concede permissão para atualizar um StreamGroup	Gravar	streamgroup*		

Tipos de recursos definidos pelo Amazon GameLift Streams

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
application	`arn:${Partition}:gameliftstreams:${Region}:${Account}:application/${ApplicationId}`	aws:ResourceTag/${TagKey}
stream group	`arn:${Partition}:gameliftstreams:${Region}:${Account}:streamgroup/${StreamGroupId}`	aws:ResourceTag/${TagKey}

Chaves de condição para Amazon GameLift Streams

O Amazon GameLift Streams define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra o acesso por uma lista de chaves da etiqueta que são permitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Global Accelerator

AWS O Global Accelerator (prefixo do serviço:`globalaccelerator`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Global Accelerator
- Tipos de recursos definidos pelo AWS Global Accelerator
- Chaves de condição do AWS Global Accelerator

Ações definidas pelo AWS Global Accelerator

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddCustomRoutingEndpoints	Concede permissão para adicionar um endpoint de sub-rede de nuvem privada virtual (VPC) a um grupo de endpoint de acelerador de roteamento personalizado	Gravar	endpointgroup*		
AddEndpoints	Concede permissão para adicionar um endpoint a um grupo de endpoints acelerador padrão	Gravar	endpointgroup*		globalaccelerator: UpdateEndpointGroup

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AdvertiseByoipCidr	Concede permissão para anunciar um intervalo de IPv4 endereços que é provisionado para uso com seu acelerador por meio de traga seus próprios endereços IP (BYOIP)	Gravar			
AllowCustomRoutingTraffic	Concede permissão para permitir o roteamento personalizado do tráfego do usuário para um IP:PORT de destino privado em uma sub-rede VPC específica	Gravar	endpointgroup*		
CreateAccelerator	Concede permissão para criar um acelerador padrão	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCrossAccountAttachment	Concede permissão para criar um CrossAccountAttachment	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateCustomRoutingAccelerator	Concede permissão para criar um acelerador de roteamento personalizado	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomRoutingEndpointGroup	Concede permissão para criar um grupo de endpoint para o listener especificado para um acelerador de roteamento personalizado	Gravar	listener*		
CreateCustomRoutingListener	Concede permissão para criar um listener para processar conexões de entrada de clientes para um acelerador de roteamento personalizado	Gravar	accelerator*		
CreateEndpointGroup	Concede permissão para adicionar um grupo de endpoint a um listener acelerador padrão	Gravar	listener*		
CreateListener	Concede permissão para adicionar um listener a um acelerador padrão	Gravar	accelerator*		
DeleteAccelerator	Concede permissão para excluir um acelerador padrão	Gravar	accelerator*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteCrossAccountAttachment	Concede permissão para excluir um CrossAccountAttachment	Gravar	attachment*		
DeleteCustomRoutingAccelerator	Concede permissão para excluir um acelerador de roteamento personalizado	Gravar	accelerator*		
DeleteCustomRoutingEndpointGroup	Concede permissão para excluir um grupo de endpoint de um listener para um acelerador de roteamento personalizado	Gravar	endpointgroup*		
DeleteCustomRoutingListener	Concede permissão para excluir um listener para um acelerador de roteamento personalizado	Gravar	listener*		
DeleteEndpointGroup	Concede permissão para excluir um grupo de endpoints associado a um listener acelerador padrão	Gravar	endpointgroup*		
DeleteListener	Concede permissão para excluir um listener de um acelerador padrão	Gravar	listener*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DenyCustomRoutingTraffic	Concede permissão para não permitir o roteamento personalizado do tráfego do usuário para um IP:PORT de destino privado em uma sub-rede VPC específica	Gravar	endpointgroup*		
DeprovisionByoipCidr	Concede permissão para liberar o intervalo de endereços especificado que você provisionou para uso com seu acelerador por meio da opção “traga seus próprios endereços IP” (BYOIP)	Gravar			
DescribeAccelerator	Concede permissões para descrever um acelerador padrão	Leitura	accelerator*		
DescribeAcceleratorAttributes	Concede permissão para descrever atributos de acelerador padrão	Leitura	accelerator*		
DescribeCrossAccountAttachment	Concede permissões para descrever um CrossAccountAttachment	Leitura	attachment*		
DescribeCustomRoutingAccelerator	Concede permissão para descrever um acelerador de roteamento personalizado	Leitura	accelerator*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeCustomRoutingAcceleratorAttributes	Concede permissão para descrever os atributos de um acelerador de roteamento personalizado	Leitura	accelerator*		
DescribeCustomRoutingEndpointGroup	Concede permissão para descrever um grupo de endpoint para um acelerador de roteamento personalizado	Leitura	endpointgroup*		
DescribeCustomRoutingListener	Concede permissão para descrever um listener para um acelerador de roteamento personalizado	Leitura	listener*		
DescribeEndpointGroup	Concede permissão para descrever um grupo de endpoint acelerador padrão	Leitura	endpointgroup*		
DescribeListener	Concede permissão para descrever um listener acelerador padrão	Leitura	listener*		
ListAccelerators	Concede permissão para listar todos os aceleradores padrão	Lista			
ListByoipCidrs	Concede permissão para listar os cidrs BYOIP	Lista			
ListCrossAccountAttachments	Concede permissão para listar tudo CrossAccountAttachments	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListCrossAccountResourceAccounts	Concede permissão para listar contas com o chamador CrossAccountAttachments listado como principal	Lista			
ListCrossAccountResources	Concede permissão para listar todos os CrossAccountAttachment recursos utilizáveis pelo chamador	Lista			
ListCustomRoutingAccelerators	Concede permissão para listar os aceleradores de roteamento personalizados para um Conta da AWS	Lista			
ListCustomRoutingEndpointGroups	Concede permissão para listar os grupos de endpoint associados a um listener para um acelerador de roteamento personalizado	Lista	listener*		
ListCustomRoutingListeners	Concede permissão para listar os listeners de um acelerador de roteamento personalizado	Lista	accelerator*		
ListCustomRoutingPortMappings	Concede permissão para listar os mapeamentos de porta para um acelerador de roteamento personalizado	Lista	accelerator*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListCustomRoutingPortMappingsByDestination	Concede permissão para listar os mapeamentos de porta para um endereço IP de um endpoint específico (um endereço de destino) em uma sub-rede	Lista			
ListEndpointGroups	Concede permissão para listar todos os grupos de endpoint associados a um listener acelerador padrão	Lista	listener*		
ListListeners	Concede permissão para listar todos os listeners associados a um acelerador padrão	Lista	accelerator*		
ListTagsForResource	Concede permissão para listar etiquetas para um recurso globalaccelerator	Leitura	accelerator		
			attachment		
ProvisionByoipCidr	Concede permissão para provisionar um intervalo de endereços para uso com seu acelerador por meio da opção “traga seus próprios endereços IP” (BYOIP)	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RemoveCustomRoutingEndpoints	Concede permissão para remover endpoints de sub-rede de nuvem privada virtual (VPC) de um grupo de endpoint de acelerador de roteamento personalizado	Gravar	endpointgroup*		
RemoveEndpoints	Concede permissão para remover um endpoint de um grupo de endpoints acelerador padrão	Gravar	endpointgroup*		globalaccelerator:UpdateEndpointGroup
TagResource	Concede permissão para adicionar etiquetas a um recurso globalaccelerator	Tags	accelerator		
			attachment		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover etiquetas de um recurso globalaccelerator	Tags	accelerator		
			attachment		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateAccelerator	Concede permissão para atualizar um acelerador padrão	Gravar	accelerator*		
UpdateAcceleratorAttributes	Concede permissão para atualizar atributos de acelerador padrão	Gravar	accelerator*		
UpdateCrossAccountAttachment	Concede permissão para atualizar um CrossAccountAttachment	Gravar	attachment*		
UpdateCustomRoutingAccelerator	Concede permissão para atualizar um acelerador de roteamento personalizado	Gravar	accelerator*		
UpdateCustomRoutingAcceleratorAttributes	Concede permissão para atualizar os atributos de um acelerador de roteamento personalizado	Gravar	accelerator*		
UpdateCustomRoutingListener	Concede permissão para atualizar um listener para um acelerador de roteamento personalizado	Gravar	listener*		
UpdateEndpointGroup	Concede permissão para atualizar um grupo de endpoints em um listener acelerador padrão	Gravar	endpointgroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateListener	Concede permissão para atualizar um listener em um acelerador padrão	Gravar	listener*		
WithdrawByoipCidr	Concede permissão para parar de anunciar um endereço BYOIP IPv4	Gravar			

Tipos de recursos definidos pelo AWS Global Accelerator

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
attachment	`arn:${Partition}:globalaccelerator::${Account}:attachment/${ResourceId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Global Accelerator

AWS O Global Accelerator define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Glue

AWS O Glue (prefixo do serviço:`glue`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.

- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Glue
- Tipos de recursos definidos pelo AWS Glue
- Chaves de condição do AWS Glue

Ações definidas pelo AWS Glue

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AuthorizeInboundIntegration [somente permissão]	Concede permissão à Glue para validar continuamente se o Arn de destino pode receber dados replicados do ARN de origem	Gravar	integration*		
BatchCreatePartition	Concede permissão para criar uma ou mais partições	Write	database*		
			rootcatalog*		
			table*		
			catalog		
BatchDeleteConnection	Concede permissão para excluir uma ou mais conexões	Write	connection*		
			rootcatalog*		
BatchDeletePartition	Concede permissão para excluir uma ou mais partições	Write	database*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			rootcatalog*		
			table*		
			catalog		
BatchDeleteTable	Concede permissão para excluir uma ou mais tabelas	Write	database*		
			rootcatalog*		
			table*		
			catalog		
BatchDeleteTableVersion	Concede permissão para excluir uma ou mais versões de uma tabela	Gravar	database*		
			rootcatalog*		
			table*		
			catalog		
BatchGetBlueprints	Concede permissão para recuperar um ou mais esquemas	Leitura	blueprint*		
BatchGetCrawlers	Concede permissão para recuperar um ou mais crawlers	Leitura	crawler*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchGetCustomEntityTypes	Concede permissão para recuperar um ou mais tipos de entidades personalizadas	Leitura			
BatchGetDevEndpoints	Concede permissão para recuperar um ou mais endpoints de desenvolvimento	Read	devendpoint*		
BatchGetJobs	Concede permissão para recuperar um ou mais trabalhos	Read	job*		
BatchGetPartition	Concede permissão para recuperar uma ou mais partições	Leitura	database*		
			rootcatalog*		
			table*		
			catalog		
BatchGetStageFiles	Concede permissão para obter arquivos de estágio em lote para o SparkUI	Gerenciamento de permissões			
BatchGetTableOptimizer	Concede permissão para retornar a configuração dos otimizadores de tabela especificados	Leitura	database*		glue:GetTable
			rootcatalog*		
			table*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchGetTriggers	Concede permissão para recuperar um ou mais triggers	Read	trigger*		
BatchGetWorkflows	Concede permissão para recuperar um ou mais fluxos de trabalho	Read	workflow*		
BatchStopJobRun	Concede permissão para interromper uma ou mais execuções de um trabalho	Gravar	job*		
BatchUpdatePartition	Concede permissão para atualizar uma ou mais partições	Gravar	database*		
			rootcatalog*		
			table*		
			catalog		
CancelDataQualityRuleRecommendationRun	Concede permissão para interromper uma execução de recomendação de uma regra de qualidade de dados em execução	Gravar	dataQualityRuleset*		
CancelDataQualityRulesetEvaluationRun	Concede permissão para interromper uma execução de avaliação de um conjunto de regras de qualidade de dados em execução	Gravar	dataQualityRuleset*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelMLTaskRun	Concede permissão para interromper a execução de uma tarefa de ML	Gravar	mlTransform*		
CancelStatement	Concede permissão para cancelar uma instrução em uma sessão interativa	Gravar	session*		
CheckSchemaVersionValidity	Concede permissão para recuperar uma verificação da validade da versão do esquema	Leitura			
CreateBlueprint	Concede permissão para criar um esquema	Gravar	blueprint*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCatalog	Concede permissão para criar um catálogo	Gravar	catalog*		
			rootcatalog*		
CreateClassifier	Concede permissão para criar um classificador.	Gravar			
CreateColumnStatisticsTaskSettings	Concede permissão para criar configurações para uma tarefa de estatísticas de coluna	Gravar	database*		
			rootcatalog*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			table*		
CreateConnection	Concede permissão para criar uma conexão	Write	rootcatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCrawler	Concede permissão para criar um crawler	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomEntityType	Concede permissão para criar tipo de entidade personalizado	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataQualityRuleset	Concede permissão para criar um conjunto de regras de qualidade de dados	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDatabase	Concede permissão para criar um banco de dados	Write	database*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			rootcatalog*		
			catalog		
CreateDevEndpoint	Concede permissão para criar um endpoint de desenvolvimento	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateGlueIdentityCenterConfiguration	Concede permissão para conectar o Glue ao Identity Center	Gravar			
CreateInboundIntegration [somente permissão]	Concede permissão ao principal de origem para criar uma integração de entrada para que os dados sejam replicados da origem para o destino	Gravar			
CreateIntegration	Concede permissão para criar uma integração	Gravar	catalog*		kms:CreateGrant kms:DescribeKey
			connection*		
			database*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			integration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIntegrationResourceProperty	Concede permissão para criar uma propriedade de recurso de integração	Gravar	catalog*		
			connection*		
			database*		
CreateIntegrationTableProperties	Concede permissão para criar propriedades da tabela de integração	Gravar	catalog*		
			connection*		
			database*		
CreateJob	Concede permissão para criar um trabalho	Write	job*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys glue:VpcIds glue:SubnetIds glue:SecurityGroupIds	
CreateMLTransform	Concede permissão para criar uma transformação de ML	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePartition	Concede permissão para criar uma partição	Gravar	database*		
			rootcatalog*		
			table*		
			catalog		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreatePartitionIndex	Concede permissão para criar um índice de partição especificado em uma tabela existente	Gravar	database*		
			rootcatalog*		
			table*		
			catalog		
CreateRegistry	Concede permissão para criar um novo registro de esquema	Write	registry*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSchema	Concede permissão para criar um novo contêiner de esquema	Write	registry*		
			schema*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateScript	Concede permissão para criar um script	Write			
CreateSecurityConfiguration	Concede permissão para criar uma configuração de segurança	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSession	Concede permissão para criar uma sessão interativa	Gravar	session*		
				aws:RequestTag/${TagKey} aws:TagKeys glue:VpcIds glue:SubnetIds glue:SecurityGroupIds	
CreateTable	Concede permissão para criar uma tabela	Gravar	database*		
			rootcatalog*		
			table*		
			catalog		
CreateTableOptimizer	Concede permissão para criar um novo otimizador de tabela para uma função específica. A compactação é o único tipo de otimizador atualmente compatível	Gravar	database*		glue:GetTable
			rootcatalog*		
			table*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateTrigger	Concede permissão para criar um trigger	Gravar	trigger*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUsageProfile	Concede permissão para criar um perfil de uso	Gravar	usageProfile*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUserDefinedFunction	Concede permissão para criar uma definição de função	Write	database*		
			rootcatalog*		
			catalog		
CreateWorkflow	Concede permissão para criar um fluxo de trabalho	Gravar	workflow*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteBlueprint	Concede permissão para excluir um esquema	Gravar	blueprint*		
DeleteCatalog	Concede permissão para excluir um catálogo	Gravar	rootcatalog*		
			catalog		
DeleteClassifier	Concede permissão para excluir um classificador	Gravar			
DeleteColumnStatisticsForPartition	Concede permissão para excluir as estatísticas de coluna de partição de uma coluna	Gravar	database*		
			rootcatalog*		
			table*		
			catalog		
DeleteColumnStatisticsForTable	Concede permissão para excluir a tabela de estatísticas de colunas	Gravar	database*		
			rootcatalog*		
			table*		
			catalog		
DeleteColumnStatisticsTaskSettings	Concede permissão para excluir configurações de uma tarefa de estatísticas de coluna	Gravar	database*		
			rootcatalog*		
			table*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteConnection	Concede permissão para excluir uma conexão	Write	connection*		
			rootcatalog*		
DeleteCrawler	Concede permissão para excluir um crawler	Gravar	crawler*		
DeleteCustomEntityType	Concede permissão para excluir tipo de entidade personalizado	Gravar			
DeleteDataQualityRuleset	Concede permissão para excluir um conjunto de regras de qualidade de dados	Gravar	dataQualityRuleset*		
DeleteDatabase	Concede permissão para excluir um banco de dados	Write	database*		
			rootcatalog*		
			table*		
			userdefinedfunction*		
			catalog		
DeleteDevEndpoint	Concede permissão para excluir um endpoint de desenvolvimento	Gravar	devendpoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteGlueIdentityCenterConfiguration	Concede permissão para desconectar o Glue do Identity Center	Gravar			
DeleteIntegration	Concede permissão para excluir uma integração	Gravar	integration*		
				aws:ResourceTag/${TagKey}	
DeleteIntegrationTableProperties	Concede permissão para excluir as propriedades da tabela de integração	Gravar	catalog*		
			connection*		
			database*		
DeleteJob	Concede permissão para excluir um trabalho	Write	job*		
DeleteMLTransform	Concede permissão para excluir uma transformação de ML	Write	mlTransform*		
DeletePartition	Concede permissão para excluir uma partição	Gravar	database*		
			rootcatalog*		
			table*		
			catalog		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeletePartitionIndex	Concede permissão para excluir um índice de partição especificado de uma tabela existente	Gravar	database*		
			rootcatalog*		
			table*		
			catalog		
DeleteRegistry	Concede permissão para excluir um registro de esquema	Write	registry*		
DeleteResourcePolicy	Concede permissão para excluir uma política de recurso	Permissions management	rootcatalog*		
DeleteSchema	Concede permissão para excluir um contêiner de esquema	Write	registry*		
			schema*		
DeleteSchemaVersions	Concede permissão para excluir um intervalo de versões de esquema	Write	registry*		
			schema*		
DeleteSecurityConfiguration	Concede permissão para excluir uma configuração de segurança	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteSession	Concede permissão para excluir uma sessão interativa após interromper a sessão, caso ainda não tenha sido interrompida	Gravar	session*		
DeleteTable	Concede permissão para excluir uma tabela	Gravar	database*		
			rootcatalog*		
			table*		
			catalog		
DeleteTableOptimizer	Concede permissão para excluir um otimizador e todos os metadados associados de uma tabela. A otimização não será mais executada na tabela	Gravar	database*		glue:GetTable
			rootcatalog*		
			table*		
DeleteTableVersion	Concede permissão para excluir uma versão de uma tabela	Write	database*		
			rootcatalog*		
			table*		
			catalog		
DeleteTrigger	Concede permissão para excluir um trigger	Gravar	trigger*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteUsageProfile	Concede permissão para excluir um perfil de uso	Gravar	usageProfile*		
DeleteUserDefinedFunction	Concede permissão para excluir uma definição de função	Write	database*		
			rootcatalog*		
			userdefinedfunction*		
			catalog		
DeleteWorkflow	Concede permissão para excluir um fluxo de trabalho	Gravar	workflow*		
DeregisterDataPreview	Concede permissão para encerrar a sessão do Glue Studio Notebook	Gerenciamento de permissões			
DescribeConnectionType	Concede permissão para descrever o tipo de conexão no Glue Studio	Gerenciamento de permissões			
DescribeEntity	Concede permissão para descrever a entidade no Glue Studio	Gerenciamento de permissões	connection*		
			rootcatalog*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeInboundIntegrations	Concede permissão para listar as integrações de entrada	Lista			
DescribeIntegrations	Concede permissão para descrever integrações sem ETL	Lista	integration*		
				aws:ResourceTag/${TagKey}	
GetBlueprint	Concede permissão para recuperar um esquema	Leitura	blueprint*		
GetBlueprintRun	Concede permissão para recuperar uma execução de esquema	Leitura	blueprint*		
GetBlueprintRuns	Concede permissão para recuperar todas as execuções de um esquema	Leitura	blueprint*		
GetCatalog	Concede permissão para recuperar um catálogo	Leitura	rootcatalog*		
			catalog		
				glue:EnabledForRedshiftAutoDiscovery	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetCatalogImportStatus	Concede permissão para recuperar o status de importação do catálogo	Leitura	rootcatalog*		
GetCatalogs	Concede permissão para recuperar todos os catálogos	Leitura	rootcatalog*		
			catalog		
				glue:EnabledForRedshiftAutoDiscovery	
GetClassifier	Concede permissão para recuperar um classificador	Read			
GetClassifiers	Concede permissão para listar todos os classificadores	Leitura			
GetColumnStatisticsForPartition	Concede permissão para recuperar estatísticas de partição de colunas	Leitura	database*		
			rootcatalog*		
			table*		
			catalog		
GetColumnStatisticsForTable	Concede permissão para recuperar a tabela de estatísticas de colunas	Leitura	database*		
			rootcatalog*		
			table*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			catalog		
GetColumnStatisticsTaskRun	Concede permissão para recuperar as informações de execução das Estatísticas de colunas para a tabela com base no run-id	Leitura			
GetColumnStatisticsTaskRuns	Concede permissão para recuperar as informações de execução das Estatísticas de colunas para a tabela com base nos run-ids	Leitura			
GetColumnStatisticsTaskSettings	Concede permissão para recuperar as configurações de uma tarefa de estatísticas de coluna	Leitura			
GetCompletion	Concede permissão para obter a resposta gerada para uma solicitação de conclusão no Glue from AWS Q	Leitura	completion*		
GetConnection	Concede permissão para recuperar uma conexão	Read	connection*		
			rootcatalog*		
GetConnections	Concede permissão para recuperar uma lista de conexões	Read	connection*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			rootcatalog*		
GetCrawler	Concede permissão para recuperar um crawler	Read	crawler*		
GetCrawlerMetrics	Concede permissão para recuperar métricas sobre crawlers	Read			
GetCrawlers	Concede permissão para recuperar todos os crawlers	Leitura			
GetCustomEntityType	Concede permissão para ler um tipo de entidade personalizada	Leitura			
GetDashboardUrl	Concede permissão para gerar um URL pré-assinado para acessar a interface do usuário do Spark Live	Leitura	session*		
GetDataCatalogEncryptionSettings	Concede permissão para recuperar as configurações de criptografia do catálogo	Leitura	rootcatalog*		
GetDataPreviewStatement	Concede permissão para obter uma instrução de pré-visualização de dados	Gerenciamento de permissões			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetDataQualityModel	Concede permissão para recuperar o status de treinamento do modelo de previsão para uma estatística	Leitura	dataQualityRuleset*		
			job*		
GetDataQualityModelResult	Concede permissão para recuperar as previsões de uma estatística do modelo mais recente	Leitura	dataQualityRuleset*		
			job*		
GetDataQualityResult	Concede permissão para recuperar um resultado de qualidade de dados	Leitura	dataQualityRuleset*		
GetDataQualityRuleRecommendationRun	Concede permissão para recuperar uma execução de recomendação de uma regra de qualidade de dados	Leitura	dataQualityRuleset*		
GetDataQualityRuleset	Concede permissão para recuperar um conjunto de regras de qualidade de dados	Leitura	dataQualityRuleset*		
GetDataQualityRulesetEvaluationRun	Concede permissão para recuperar uma execução de recomendação de uma regra de qualidade de dados	Leitura	dataQualityRuleset*		
GetDatabase	Concede permissão para recuperar um banco de dados	Read	database*		
			rootcatalog*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			catalog		
GetDatabases	Concede permissão para recuperar todos os bancos de dados	Read	database*		
			rootcatalog*		
			catalog		
GetDataflowGraph	Concede permissão para transformar um script em um gráfico acíclico dirigido (DAG, directed acyclic graph)	Read			
GetDevEndpoint	Concede permissão para recuperar um endpoint de desenvolvimento	Read	devendpoint*		
GetDevEndpoints	Concede permissão para recuperar todos os endpoints de desenvolvimento	Leitura			
GetEntityRecords	Concede permissão para visualizar registros de entidades no Glue	Leitura	catalog*		
			connection		
GetEnvironment	Concede permissão para obter detalhes do ambiente do SparkUI	Gerenciamento de permissões			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetExecutors	Concede permissão para obter executores para o SparkUI	Gerenciamento de permissões			
GetExecutorsThreads	Concede permissão para obter threads de executor para o SparkUI	Gerenciamento de permissões			
GetGeneratedCode	Transforma um gráfico acíclico direcionado (DAG) em código	Leitura			
GetGlueIdentityCenterConfiguration	Concede permissão para recuperar o aplicativo Idc gerenciado	Leitura			
GetIntegrationResourceProperty	Concede permissão para recuperar a propriedade do recurso de integração	Leitura	catalog*		
			connection*		
			database*		
GetIntegrationTableProperties	Concede permissão para recuperar as propriedades da tabela de integração	Leitura	catalog*		
			connection*		
			database*		
GetJob	Concede permissão para recuperar um trabalho	Read	job*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetJobBookmark	Concede permissão para recuperar um marcador de trabalho	Read			
GetJobRun	Concede permissão para recuperar a execução de um trabalho	Read	job*		
GetJobRuns	Concede permissão para recuperar todas as execuções de um trabalho	Leitura	job*		
GetJobUpgradeAnalysis	Concede permissão para recuperar uma análise de atualização para um trabalho	Leitura	job*		
GetJobs	Concede permissão para recuperar todos os trabalhos atuais	Leitura			
GetLogParsingStatus	Concede permissão para obter o status de análise de log para o SparkUI	Gerenciamento de permissões			
GetMLTaskRun	Concede permissão para recuperar uma execução de tarefa de ML	Read	mlTransform*		
GetMLTaskRuns	Concede permissão para recuperar todas as execuções de tarefas de ML	List	mlTransform*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetMLTransform	Concede permissão para recuperar uma transformação de ML	Read	mlTransform*		
GetMLTransforms	Concede permissão para recuperar todas as transform ações de ML	List	mlTransform*		
GetMapping	Concede permissão para criar um mapeamento	Leitura			
GetNotebookInstanceStatus	Concede permissão para recuperar o status da sessão do Glue Studio Notebooks	Gerenciamento de permissões			
GetPartition	Concede permissão para recuperar uma partição	Leitura	database*		
			rootcatalog*		
			table*		
			catalog		
GetPartitionIndexes	Concede permissão para recuperar os índices de partições de uma tabela	Leitura	database*		
			rootcatalog*		
			table*		
			catalog		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetPartitions	Concede permissão para recuperar as partições de uma tabela	Read	database*		
			rootcatalog*		
			table*		
			catalog		
GetPlan	Concede permissão para recuperar um mapeamento para um script	Leitura			
GetQueries	Concede permissão para obter consultas para o SparkUI	Gerenciamento de permissões			
GetQuery	Concede permissão para obter uma consulta específica para o SparkUI	Gerenciamento de permissões			
GetRecipeAction	Concede permissão para obter o resultado de uma declaração de fórmula de preparação de dados	Gerenciamento de permissões			
GetRegistry	Concede permissão para recuperar um registro de esquema	Read	registry*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetResourcePolicies	Concede permissão para recuperar políticas de recursos	Read	rootcatalog*		
GetResourcePolicy	Concede permissão para recuperar uma política de recurso	Read	rootcatalog*		
GetSchema	Concede permissão para recuperar um contêiner de esquema	Read	registry*		
			schema*		
GetSchemaByDefinition	Concede permissão para recuperar uma versão de esquema com base na definição do esquema	Read	registry*		
			schema*		
GetSchemaVersion	Concede permissão para recuperar uma versão de esquema	Read	registry		
			schema		
GetSchemaVersionsDiff	Concede permissão para comparar duas versões de esquema no registro do esquema	Read	registry*		
			schema*		
GetSecurityConfiguration	Concede permissão para recuperar uma configuração de segurança	Read			
GetSecurityConfigurations	Concede permissão para recuperar uma ou mais configurações de segurança	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSession	Concede permissão para recuperar uma sessão interativa	Leitura	session*		
GetStage	Concede permissão para obter um estágio para o SparkUI	Gerenciamento de permissões			
GetStageAttempt	Concede permissão para obter uma tentativa de estágio para o SparkUi	Gerenciamento de permissões			
GetStageAttemptTaskList	Concede permissão para obter a lista de tarefas para uma tentativa de estágio para o SparkUI	Gerenciamento de permissões			
GetStageAttemptTaskSummary	Concede permissão para obter o resumo da tarefa de uma tentativa de estágio para o SparkUI	Gerenciamento de permissões			
GetStageFiles	Concede permissão para obter arquivos de estágio para o SparkUI	Gerenciamento de permissões			
GetStages	Concede permissão para obter estágios para o SparkUI	Gerenciamento de permissões			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetStatement	Concede permissão para recuperar resultados e informações sobre uma instrução de uma sessão interativa	Leitura	session*		
GetStorage	Concede permissão para obter os detalhes de armazenamento do SparkUI	Gerenciamento de permissões			
GetStorageUnit	Concede permissão para obter os detalhes da unidade de armazenamento do SparkUI	Gerenciamento de permissões			
GetTable	Concede permissão para recuperar uma tabela	Leitura	database*		
			rootcatalog*		
			table*		
			catalog		
GetTableOptimizer	Concede permissão para retornar a configuração de todos os otimizadores associados a uma tabela especificada	Leitura	database*		glue:GetTable
			rootcatalog*		
			table*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetTableVersion	Concede permissão para recuperar uma versão de uma tabela	Read	database*		
			rootcatalog*		
			table*		
			catalog		
GetTableVersions	Concede permissão para recuperar uma lista de versões de uma tabela	Read	database*		
			rootcatalog*		
			table*		
			catalog		
GetTables	Concede permissão para recuperar as tabelas em um banco de dados	Read	database*		
			rootcatalog*		
			table*		
			catalog		
GetTags	Concede permissão para recuperar todas as etiquetas associadas a um recurso	Read	blueprint		
			crawler		
			customEntityType		
			devendpoint		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			job		
			trigger		
			usageProfile		
			workflow		
GetTrigger	Concede permissão para recuperar um trigger	Read	trigger*		
GetTriggers	Concede permissão para recuperar os triggers associados a um trabalho	Leitura			
GetUsageProfile	Concede permissão para recuperar um perfil de uso	Leitura	usageProfile*		
GetUserDefinedFunction	Concede permissão para recuperar uma definição de função	Leitura	database*		
			rootcatalog*		
			userdefinedfunction*		
			catalog		
GetUserDefinedFunctions	Concede permissão para recuperar várias definições de função	Read	database*		
			rootcatalog*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			userdefinedfunction*		
			catalog		
GetWorkflow	Concede permissão para recuperar um fluxo de trabalho	Read	workflow*		
GetWorkflowRun	Concede permissão para recuperar uma execução de fluxo de trabalho	Read	workflow*		
GetWorkflowRunProperties	Concede permissão para recuperar propriedades de execução de fluxo de trabalho	Read	workflow*		
GetWorkflowRuns	Concede permissão para recuperar todas as execuções de um fluxo de trabalho	Leitura	workflow*		
GlueNotebookAuthorize	Concede permissão para acessar o Glue Studio Notebooks	Gerenciamento de permissões			
GlueNotebookRefreshCredentials	Concede permissão para atualizar as credenciais do Glue Studio Notebooks	Gerenciamento de permissões			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ImportCatalogToGlue	Concede permissão para importar um catálogo de dados do Athena para o Glue AWS	Gravar	rootcatalog*		
ListBlueprints	Concede permissão para recuperar todos os esquemas	Lista			
ListColumnStatisticsTaskRuns	Concede permissão para listar todos os run-ids das Estatísticas de colunas que foram executadas para a conta	Leitura			
ListConnectionTypes	Concede permissão para listar tipos de conexão no Glue Studio	Gerenciamento de permissões			
ListCrawlers	Concede permissão para recuperar todos os crawlers	Lista			
ListCrawls	Concede permissão para recuperar o histórico de crawler	Lista	crawler*		
ListCustomEntityTypes	Concede permissão para recuperar todos os tipos de entidades personalizadas	Lista			
ListDataQualityResults	Concede permissão para recuperar todos os resultados de qualidade de dados	Lista	dataQualityRuleset*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDataQualityRulesetRecommendationRuns	Concede permissão para recuperar todas as execuções de recomendação de uma regra de qualidade de dados	Lista	dataQualityRuleset*		
ListDataQualityRulesetEvaluationRuns	Concede permissão para recuperar todas as execuções de recomendação de uma regra de qualidade de dados	Lista	dataQualityRuleset*		
ListDataQualityRulesets	Concede permissão para recuperar uma lista de conjuntos de regras de qualidade de dados	Lista	dataQualityRuleset*		
ListDevEndpoints	Concede permissão para recuperar todos os endpoints de desenvolvimento	Lista			
ListEntities	Concede permissão para listar as entidades no Glue Studio	Gerenciamento de permissões	connection* rootcatalog*		
ListJobUpgradeAnalyses	Concede permissão para listar análises de atualização para um trabalho	Lista	job*		
ListJobs	Concede permissão para recuperar todos os trabalhos atuais	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListMLTransforms	Concede permissão para recuperar todas as transformações de ML	List	mlTransform*		
ListRegistries	Concede permissão para recuperar uma lista de registros de esquema	List			
ListSchemaVersions	Concede permissão para recuperar uma lista de versões de esquema	List	registry*		
			schema*		
ListSchemas	Concede permissão para recuperar uma lista de contêineres de esquema	Lista	registry		
ListSessions	Concede permissão para recuperar uma lista de sessão interativa	Lista			
ListStatements	Concede permissão para recuperar uma lista de instruções de uma sessão interativa	Lista	session*		
ListTableOptimizerRuns	Concede permissão para listar o histórico de execuções anteriores do otimizador para uma tabela específica	Lista	database*		glue:GetTable
			rootcatalog*		
			table*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTriggers	Concede permissão para recuperar todos os triggers	Lista			
ListUsageProfiles	Concede permissão para recuperar uma lista de perfis de uso	Lista			
ListWorkflows	Concede permissão para recuperar todos os fluxos de trabalho	Lista			
ModifyIntegration	Concede permissão para modificar uma integração com zero ETL	Gravar	integration*		
				aws:ResourceTag/${TagKey}	
NotifyEvent	Concede permissão para notificar de um evento o fluxo de trabalho orientado por evento	Gravar	workflow*		
PassConnection [somente permissão]	Concede permissão para passar o nome da conexão de cola na entrada para APIs que os exija	Gravar	connection*		
PublishDataQuality [somente permissão]	Concede permissão para publicar resultados de qualidade de dados	Gravar	dataQualityRuleset*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutDataCatalogEncryptionSettings	Concede permissão para atualizar as configurações de criptografia do catálogo	Gravar	rootcatalog*		
PutDataQualityProfileAnnotation	Concede permissão para anotar todos os pontos de dados de um perfil	Gravar	dataQualityRuleset*		
			job*		
PutDataQualityStatisticAnnotation	Concede permissão para anotar pontos de dados ao longo do tempo para uma estatística específica de qualidade de dados	Gravar	dataQualityRuleset*		
			job*		
PutResourcePolicy	Concede permissão para atualizar uma política de recurso	Permissions management	rootcatalog*		
PutSchemaVersionMetadata	Concede permissão para adicionar metadados à versão do esquema	Write	registry		
			schema		
PutWorkflowRunProperties	Concede permissão para atualizar propriedades de execução de fluxo de trabalho	Write	workflow*		
QuerySchemaVersionMetadata	Concede permissão para buscar metadados para uma versão de esquema	Lista	registry		
			schema		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RefreshOAuth2Tokens	Concede permissão para atualizar os tokens OAuth2 para conexão durante a execução do trabalho	Gerenciamento de permissões	connection*		
			rootcatalog*		
RegisterSchemaVersion	Concede permissão para criar uma nova versão de esquema	Write	registry*		
			schema*		
RemoveSchemaVersionMetadata	Concede permissão para remover metadados da versão do esquema	Gravar	registry		
			schema		
RequestLogParsing	Concede permissão para solicitar análise de log para o SparkUI	Gerenciamento de permissões			
ResetJobBookmark	Concede permissão para redefinir um marcador de trabalho	Write			
ResumeWorkflowRun	Concede permissão para retomar uma execução de fluxo de trabalho	Gravar	workflow*		
RunDataPreviewStatement	Concede permissão para executar uma instrução de pré-visualização de dados	Gerenciamento de permissões			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RunStatement	Concede permissão para executar um código ou uma instrução em uma sessão interativa	Gravar	session*		
SearchTables	Concede permissão para recuperar as tabelas no catálogo	Leitura	database*		
			rootcatalog*		
			table*		
			catalog		
SendFeedback	Concede permissão para fornecer feedback sobre uma experiência de preenchimento com cola em AWS Q	Gravar			
SendRecipeAction	Concede permissão para executar uma declaração de fórmula de preparação de dados na visualização de dados	Gerenciamento de permissões			
StartBlueprintRun	Concede permissão para iniciar a execução de um esquema	Gravar	blueprint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartColumnStatisticsTaskRun	Concede permissão para iniciar uma execução para gerar Estatísticas de colunas para a tabela	Gravar	database*		glue:GetSecurityConfiguration glue:GetTable
			rootcatalog*		
			table*		
StartColumnStatisticsTaskRunSchedule	Concede permissão para iniciar um cronograma de execução de tarefas de estatísticas de coluna	Gravar	database*		
			rootcatalog*		
			table*		
StartCompletion	Concede permissão para criar uma solicitação de conclusão na experiência Glue for AWS Q	Gravar			
StartCrawler	Concede permissão para iniciar um crawler	Write	crawler*		
StartCrawlerSchedule	Concede permissão para alterar o estado da programação de um crawler para SCHEDULED (programado)	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartDataQualityRuleRecommendationRun	Concede permissão para iniciar uma execução de recomendação de uma regra de qualidade de dados	Gravar	dataQualityRuleset*		
StartDataQualityRulesetEvaluationRun	Concede permissão para iniciar uma execução de recomendação de uma regra de qualidade de dados	Gravar	dataQualityRuleset*		
StartExportLabelsTaskRun	Concede permissão para iniciar uma execução de tarefa de ML de exportação de rótulos	Write	mlTransform*		
StartImportLabelsTaskRun	Concede permissão para iniciar uma execução de tarefa de ML de importação de rótulos	Write	mlTransform*		
StartJobRun	Concede permissão para iniciar a execução de um trabalho	Gravar	job*		
StartJobUpgradeAnalysis	Concede permissão para começar a executar a análise de atualização de um trabalho	Gravar	job*		
StartMLEvaluationTaskRun	Concede permissão para iniciar uma execução de tarefa de ML de avaliação	Write	mlTransform*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartMLLabelingSetGenerationTaskRun	Concede permissão para iniciar uma execução de tarefa de ML da geração do conjunto de rótulos	Gravar	mlTransform*		
StartNotebook	Concede permissão para iniciar o Glue Studio Notebooks	Gerenciamento de permissões			
StartTrigger	Concede permissão para iniciar um trigger	Write	trigger*		
StartWorkflowRun	Concede permissão para iniciar a execução de um fluxo de trabalho	Gravar	workflow*		
StopColumnStatisticsTaskRun	Concede permissão para interromper a execução de Estatísticas de colunas	Gravar	database*		
			rootcatalog*		
			table*		
StopColumnStatisticsTaskRunSchedule	Concede permissão para interromper o cronograma de execução de tarefas de estatísticas de uma coluna	Gravar	database*		
			rootcatalog*		
			table*		
StopCrawler	Concede permissão para interromper um crawler em execução	Write	crawler*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopCrawlerSchedule	Concede permissão para definir o estado de programação de um crawler para NOT_SCHEDULED (não programado)	Gravar			
StopJobUpgradeAnalysis	Concede permissão para interromper uma análise de atualização contínua de um trabalho	Gravar	job*		
StopSession	Concede permissão para interromper uma sessão interativa	Gravar	session*		
StopTrigger	Concede permissão para interromper um trigger	Write	trigger*		
StopWorkflowRun	Concede permissão para interromper uma execução de fluxo de trabalho	Write	workflow*		
TagResource	Concede permissão para adicionar tags a um recurso	Tags	blueprint		
			connection		
			crawler		
			customEntityType		
			dataQualityRuleset		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			devendpoint		
			integration		
			job		
			mlTransform		
			registry		
			schema		
			session		
			trigger		
			usageProfile		
			workflow		
				aws:TagKeys aws:RequestTag/${TagKey}	
Terminate Notebook	Concede permissão para encerrar o Glue Studio Notebooks	Gerenciamento de permissões			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TestConnection	Concede permissão para testar a conexão no Glue Studio	Gerenciamento de permissões			
UntagResource	Concede permissão para remover etiquetas associadas a um recurso	Tags	blueprint		
			connection		
			crawler		
			customEntityType		
			dataQualityRuleset		
			devendpoint		
			integration		
			job		
			mlTransform		
			registry		
			schema		
			session		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			trigger		
			usageProfile		
			workflow		
				aws:TagKeys	
UpdateBlueprint	Concede permissão para atualizar um esquema	Gravar	blueprint*		
UpdateCatalog	Concede permissão para atualizar um catálogo	Gravar	rootcatalog*		
			catalog		
UpdateClassifier	Concede permissão para atualizar um classificador	Gravar			
UpdateColumnStatisticsForPartition	Concede permissão para atualizar estatísticas de partição de colunas	Gravar	database*		
			rootcatalog*		
			table*		
			catalog		
UpdateColumnStatisticsForTable	Concede permissão para atualizar a tabela de estatísticas de colunas	Gravar	database*		
			rootcatalog*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			table*		
			catalog		
UpdateColumnStatisticsTaskSettings	Concede permissão para atualizar as configurações de uma tarefa de estatísticas de coluna	Gravar	database*		
			rootcatalog*		
			table*		
UpdateConnection	Concede permissão para atualizar uma conexão	Write	connection*		
			rootcatalog*		
UpdateCrawler	Concede permissão para atualizar um crawler	Write	crawler*		
UpdateCrawlerSchedule	Concede permissão para atualizar a programação de um crawler	Gravar			
UpdateDataQualityRuleset	Concede permissão para atualizar um conjunto de regras de qualidade de dados	Gravar	dataQualityRuleset*		
UpdateDatabase	Concede permissão para atualizar um banco de dados	Write	database*		
			rootcatalog*		
			catalog		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateDevEndpoint	Concede permissão para atualizar um endpoint de desenvolvimento	Gravar	devendpoint*		
UpdateGlueIdentityCenterConfiguration	Concede permissão para atualizar o aplicativo Idc gerenciado	Gravar			
UpdateIntegrationResourceProperty	Concede permissão para atualizar a propriedade do recurso de integração	Gravar	catalog*		
			connection*		
			database*		
UpdateIntegrationTableProperties	Concede permissão para atualizar as propriedades da tabela de integração	Gravar	catalog*		
			connection*		
			database*		
UpdateJob	Concede permissão para atualizar um trabalho	Gravar	job*		
				glue:VpcIds glue:SubnetIds glue:SecurityGroupIds	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateJobFromSourceControl	Concede permissão para atualizar um trabalho a partir do provedor de controle de origem	Gravar	job*		
UpdateMLTransform	Concede permissão para atualizar uma transformação de ML	Write	mlTransform*		
UpdatePartition	Concede permissão para atualizar uma partição	Write	database*		
			rootcatalog*		
			table*		
			catalog		
UpdateRegistry	Concede permissão para atualizar um registro de esquema	Write	registry*		
UpdateSchema	Concede permissão para atualizar um contêiner de esquema	Gravar	registry*		
			schema*		
UpdateSourceControlFromJob	Concede permissão para atualizar um provedor de controle de origem a partir de um trabalho	Gravar	job*		
UpdateTable	Concede permissão para atualizar uma tabela	Gravar	database*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			rootcatalog*		
			table*		
			catalog		
UpdateTableOptimizer	Concede permissão para atualizar a configuração de um otimizador de tabela existente	Gravar	database*		glue:GetTable
			rootcatalog*		
			table*		
UpdateTrigger	Concede permissão para atualizar um trigger	Gravar	trigger*		
UpdateUsageProfile	Concede permissão para atualizar um perfil de uso	Gravar	usageProfile*		
UpdateUserDefinedFunction	Concede permissão para atualizar uma definição de função	Write	database*		
			rootcatalog*		
			userdefinedfunction*		
			catalog		
UpdateWorkflow	Concede permissão para atualizar um fluxo de trabalho	Gravar	workflow*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpgradeJob	Concede permissão para atualizar um trabalho para a versão mais recente	Gravar	job*		
UseGlueStudio	Concede permissão para usar o Glue Studio e acessar seu conteúdo interno APIs	Gerenciamento de permissões			
UseMLTransforms [somente permissão]	Concede permissão para usar uma transformação de ML de dentro de um script de ETL do Glue	Write	mlTransform*		

Tipos de recursos definidos pelo AWS Glue

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
rootcatalog	`arn:${Partition}:glue:${Region}:${Account}:catalog`	
catalog	`arn:${Partition}:glue:${Region}:${Account}:catalog/${CatalogName}`	

Tipos de recursos	ARN	Chaves de condição
database	arn:${Partition}:glue:${Region}:${Account}:database/${DatabaseName}	
table	arn:${Partition}:glue:${Region}:${Account}:table/${DatabaseName}/${TableName}	
tableversion	arn:${Partition}:glue:${Region}:${Account}:tableVersion/${DatabaseName}/${TableName}/${TableVersionName}	
connection	arn:${Partition}:glue:${Region}:${Account}:connection/${ConnectionName}	aws:ResourceTag/${TagKey}
userdefinedfunction	arn:${Partition}:glue:${Region}:${Account}:userDefinedFunction/${DatabaseName}/${UserDefinedFunctionName}	
devendpoint	arn:${Partition}:glue:${Region}:${Account}:devEndpoint/${DevEndpointName}	aws:ResourceTag/${TagKey}
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}

Tipos de recursos	ARN	Chaves de condição
mlTransform	arn:${Partition}:glue:${Region}:${Account}:mlTransform/${TransformId}	aws:ResourceTag/${TagKey}
registry	arn:${Partition}:glue:${Region}:${Account}:registry/${RegistryName}	aws:ResourceTag/${TagKey}
schema	arn:${Partition}:glue:${Region}:${Account}:schema/${SchemaName}	aws:ResourceTag/${TagKey}
session	arn:${Partition}:glue:${Region}:${Account}:session/${SessionId}	aws:ResourceTag/${TagKey}
usageProfile	arn:${Partition}:glue:${Region}:${Account}:usageProfile/${UsageProfileId}	aws:ResourceTag/${TagKey}
dataQualityRuleset	arn:${Partition}:glue:${Region}:${Account}:dataQualityRuleset/${RulesetName}	aws:ResourceTag/${TagKey}
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}

Chaves de condição do AWS Glue

AWS Glue define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as

quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString
glue:CredentialIssuingService	Filtra o acesso pelo serviço a partir do qual as credencia is da solicitação são emitidas	String
glue:EnabledForRedshiftAutoDiscovery	Filtra o acesso pela presença da chave configurada para a política baseada em identidade da função	Bool
glue:RoleAssumedBy	Filtra o acesso pelo serviço a partir do qual as credencia is da solicitação são obtidas assumindo a função de cliente	String
glue:SecurityGroupIds	Filtra o acesso pelo ID de grupos de segurança configura dos para o trabalho do Glue	ArrayOfString
glue:SubnetIds	Filtra o acesso pelo ID de sub-redes configuradas para o trabalho do Glue	ArrayOfString

Chaves de condição	Descrição	Tipo
glue:VpcIds	Filtra o acesso pelo ID da VPC configurada para o trabalho do Glue	ArrayOfString

Ações, recursos e chaves de condição para AWS Glue DataBrew

AWS O Glue DataBrew (prefixo do serviço:`databrew`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Glue DataBrew
- Tipos de recursos definidos pelo AWS Glue DataBrew
- Teclas de condição para AWS Glue DataBrew

Ações definidas pelo AWS Glue DataBrew

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchDeleteRecipeVersion	Concede permissão para excluir uma ou mais versões de receita	Write	Recipe*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDataset	Concede permissão para criar um conjunto de dados	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateProfileJob	Concede permissão para criar um trabalho de perfil	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateProject	Concede permissão para criar um projeto	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateRecipe	Concede permissão para criar uma receita	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateRecipeJob	Concede permissão para criar um trabalho de receita	Gravar		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateRuleset	Concede permissão para criar um conjunto de regras	Gravar		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSchedule	Concede permissão para criar um agendamento	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeleteDataset	Concede permissão para excluir um conjunto de dados	Write	Dataset*		
DeleteJob	Concede permissão para excluir um trabalho	Write	Job*		
DeleteProject	Concede permissão para excluir um projeto	Write	Project*		
DeleteRecipeVersion	Concede permissão para excluir uma versão de receita	Gravar	Recipe*		
DeleteRuleset	Concede permissão para excluir um grupo de regras	Gravar	Ruleset*		
DeleteSchedule	Concede permissão para excluir um agendamento	Write	Schedule*		
DescribeDataset	Concede permissão para exibir detalhes sobre um conjunto de dados	Read	Dataset*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeJob	Concede permissão para exibir detalhes sobre um trabalho	Read	Job*		
DescribeJobRun	Concede permissão para exibir detalhes sobre a execução do trabalho para um determinado trabalho	Read	Job*		
DescribeProject	Concede permissão para visualizar detalhes sobre um projeto	Read	Project*		
DescribeRecipe	Concede permissão para visualizar detalhes sobre uma receita	Leitura	Recipe*		
DescribeRuleset	Concede permissão para exibir detalhes sobre um conjunto de regras	Leitura	Ruleset*		
DescribeSchedule	Concede permissão para visualizar detalhes sobre um agendamento	Read	Schedule*		
ListDatasets	Concede permissão para listar conjuntos de dados em sua conta	Read			
ListJobRuns	Concede permissão para listar execuções de tarefas para um determinado trabalho	Read	Job*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListJobs	Concede permissão para listar trabalhos na sua conta	Read			
ListProjects	Concede permissão para listar projetos em sua conta	Read			
ListRecipeVersions	Concede permissão para listar versões em sua receita	Read	Recipe*		
ListRecipes	Concede permissão para listar receitas em sua conta	Leitura			
ListRulesets	Concede permissão para listar conjuntos de regras na sua conta	Leitura			
ListSchedules	Concede permissão para listar agendamentos na sua conta	Read			
ListTagsForResource	Concede permissão para recuperar etiquetas associadas a um recurso	Read	Dataset		
			Job		
			Project		
			Recipe		
			Ruleset		
			Schedule		
PublishRecipe	Concede permissão para publicar uma grande versão de uma receita	Write	Recipe*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SendProjectSessionAction	Concede permissão para enviar uma ação para a sessão interativa de um projeto	Write	Project*		
StartJobRun	Concede permissão para iniciar a execução de um trabalho	Write	Job*		
StartProjectSession	Concede permissão para iniciar uma sessão interativa para um projeto	Write	Project*		
StopJobRun	Concede permissão para interromper uma execução de trabalho para um trabalho	Write	Job*		
TagResource	Concede permissão para adicionar tags a um recurso	Marcação	Dataset		
			Job		
			Project		
			Recipe		
			Ruleset		
			Schedule		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover etiquetas associadas a um recurso	Marcação	Dataset		
			Job		
			Project		
			Recipe		
			Ruleset		
			Schedule		
				aws:TagKeys	
UpdateDataset	Concede permissão para modificar um conjunto de dados	Write	Dataset*		
UpdateProfileJob	Concede permissão para modificar um trabalho de perfil	Write	Job*		
UpdateProject	Concede permissão para modificar um projeto	Write	Project*		
UpdateRecipe	Concede permissão para modificar uma receita	Write	Recipe*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateRecipeJob	Concede permissão para modificar um trabalho de receita	Gravar	Job*		
UpdateRuleset	Concede permissão para modificar um conjunto de regras	Gravar	Ruleset*		
UpdateSchedule	Concede permissão para modificar um agendamento	Gravar	Schedule*		

Tipos de recursos definidos pelo AWS Glue DataBrew

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Tipos de recursos	ARN	Chaves de condição
Recipe	`arn:${Partition}:databrew:${Region}:${Account}:recipe/${ResourceId}`	aws:ResourceTag/${TagKey}
Job	`arn:${Partition}:databrew:${Region}:${Account}:job/${ResourceId}`	aws:ResourceTag/${TagKey}
Schedule	`arn:${Partition}:databrew:${Region}:${Account}:schedule/${ResourceId}`	aws:ResourceTag/${TagKey}

Teclas de condição para AWS Glue DataBrew

AWS Glue DataBrew define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Ground Station

AWS O Ground Station (prefixo do serviço:`groundstation`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Ground Station
- Tipos de recursos definidos pelo AWS Ground Station
- Chaves de condição do AWS Ground Station

Ações definidas pelo AWS Ground Station

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelContact	Concede permissão para cancelar um contato	Write	Contact*		
CreateConfig	Concede permissão para criar uma configuração	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataflowEndpointGroup	Concede permissão para criar um grupo de endpoints de fluxo de dados	Gravar		aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
CreateEphemeris	Concede permissão para criar um item efêmero	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateMissionProfile	Concede permissão para criar um perfil de missão	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfig	Concede permissão para excluir um config	Write	Config*		
DeleteDataflowEndpointGroup	Concede permissão para excluir um grupo de endpoints de fluxo de dados	Gravar	DataflowEndpointGroup*		
DeleteEphemeris	Concede permissão para excluir um item efêmero	Gravar	EphemerisItem*		
DeleteMissionProfile	Concede permissão para excluir um perfil de missão	Write	MissionProfile*		
DescribeContact	Concede permissão para descrever um contato	Leitura	Contact*		
DescribeEphemeris	Concede permissão para descrever um item efêmero	Leitura	EphemerisItem*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAgentConfiguration	Concede permissão para obter a configuração de um atendente	Leitura	Agent*		
GetConfig	Concede permissão para retornar uma configuração	Read	Config*		
GetDataflowEndpointGroup	Concede permissão para retornar um grupo de endpoints de fluxo de dados	Read	DataflowEndpointGroup*		
GetMinuteUsage	Concede permissão para retornar o uso de minutos	Read			
GetMissionProfile	Concede permissão para recuperar um perfil de missão	Read	MissionProfile*		
GetSatellite	Concede permissão para retornar informações sobre um satélite	Read	Satellite*		
ListConfigs	Concede permissão para retornar uma lista de configurações anteriores	List			
ListContacts	Concede permissão para retornar uma lista de contatos	List			
ListDataflowEndpointGroups	Concede permissão para listar grupos de endpoints de fluxo de dados	Lista			
ListEphemerides	Concede permissão para listar itens efêmeros	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListGroundStations	Concede permissão para listar estações terrestres	List			
ListMissionProfiles	Concede permissão para retornar uma lista de perfis de missão	List			
ListSatellites	Concede permissão para listar satélites	List			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	Config		
			Contact		
			DataflowEndpointGroup		
			MissionProfile		
RegisterAgent	Concede permissão para registrar um atendente	Gravar			
ReserveContact	Concede permissão para reservar um contato	Write		aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Concede permissão para atribuir uma tag de recurso	Tags	Config		
			Contact		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			DataflowEndpointGroup		
			EphemerisItem		
			MissionProfile		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para cancelar a atribuição uma tag de recurso	Tags	Config		
			Contact		
			DataflowEndpointGroup		
			EphemerisItem		
			MissionProfile		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateAgentStatus	Concede permissão para atualizar o status de um atendente	Gravar	Agent*		
UpdateConfig	Concede permissão para atualizar uma configuração	Gravar	Config*		
UpdateEphemeris	Concede permissão para atualizar um item efêmero	Gravar	EphemerisItem*		
UpdateMissionProfile	Concede permissão para atualizar um perfil de missão	Write	MissionProfile*		

Tipos de recursos definidos pelo AWS Ground Station

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
Config	`arn:${Partition}:groundstation:${Region}:${Account}:config/${ConfigType}/${ConfigId}`	aws:ResourceTag/${TagKey} groundstation:ConfigId

Tipos de recursos	ARN	Chaves de condição
		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

Chaves de condição do AWS Ground Station

AWS O Ground Station define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString
groundstation:AgentId	Filtra o acesso pelo ID de um atendente	String
groundstation:ConfigId	Filtra o acesso pelo ID de um config	String
groundstation:ConfigType	Filtra o acesso pelo tipo de um config	String
groundstation:ContactId	Filtra o acesso pelo ID de um contato	String
groundstation:DataflowEndpointGroupId	Filtra o acesso pelo ID de um grupo de endpoints de fluxo de dados	String

Chaves de condição	Descrição	Tipo
groundstation:EphemerisId	Filtra o acesso pelo ID de uma item efêmero	String
groundstation:GroundStationId	Filtra o acesso pelo ID de uma ground station	String
groundstation:MissionProfileId	Filtra o acesso pelo ID de um perfil de missão	String
groundstation:SatelliteId	Filtra o acesso pelo ID de um satélite	String

Ações, recursos e chaves de condição para a Amazon GroundTruth Labeling

A Amazon GroundTruth Labeling (prefixo do serviço:`groundtruthlabeling`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon GroundTruth Labeling
- Tipos de recursos definidos pela Amazon GroundTruth Labeling
- Chaves de condição para Amazon GroundTruth Labeling

Ações definidas pela Amazon GroundTruth Labeling

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociatePatchToManifestJob [somente permissão]	Concede permissão para associar um arquivo de patch ao arquivo manifesto para atualizar o arquivo manifesto	Write			
CreateBatch [somente permissão]	Concede permissão para criar um GT Batch	Gravar			
CreateIntakeForm [somente permissão]	Concede permissão para criar um formulário de admissão	Gravar			
CreateProject [somente permissão]	Concede permissão para criar um projeto GT	Gravar			
CreateWorkflowDefinition [somente permissão]	Concede permissão para criar uma definição de fluxo de trabalho do GT	Gravar			
DescribeConsoleJob [somente permissão]	Concede permissão para obter o status de GroundTruthLabeling Empregos	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GenerateLIDARPreviewTaskConfigJob [somente permissão]	Concede permissão para gerar uma tarefa de visualização do LiDAR	Gravar			
GetBatch [somente permissão]	Concede permissão para obter um GT Batch	Leitura			
GetIntakeFormStatus [somente permissão]	Concede permissão para obter formulários de admissão	Leitura			
ListBatches [somente permissão]	Concede permissão para listar um GT Batchs	Leitura			
ListDatasetObjects [somente permissão]	Concede permissão para listar objetos de conjunto de dados em um arquivo manifesto	Read			
ListProjects [somente permissão]	Concede permissão para listar projetos do GT	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RunFilterOrSampleDatasetJob [somente permissão]	Concede permissão para filtrar registros de um arquivo manifesto usando o S3 Select. Obtenha exemplos de entradas com base em amostragem aleatória	Write			
RunGenerateManifestByCrawlingJob [somente permissão]	Concede permissão para listar um prefixo do S3 e criar arquivos manifesto de objetos nesse local	Gravar			
RunGenerateManifestMetricsJob [somente permissão]	Concede permissão para gerar métricas usando objetos no manifesto	Gravar			
UpdateBatch [somente permissão]	Concede permissão para atualizar um GT Batch	Gravar			

Tipos de recursos definidos pela Amazon GroundTruth Labeling

A Amazon GroundTruth Labeling não suporta a especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para permitir o acesso à Amazon GroundTruth Labeling, especifique `"Resource": "*"` em sua política.

Chaves de condição para Amazon GroundTruth Labeling

GroundTruth A rotulagem não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para a Amazon GuardDuty

A Amazon GuardDuty (prefixo do serviço:`guardduty`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon GuardDuty
- Tipos de recursos definidos pela Amazon GuardDuty
- Chaves de condição para a Amazon GuardDuty

Ações definidas pela Amazon GuardDuty

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptAdministratorInvitation	Concede permissão para aceitar convites para se tornar uma conta de membro GuardDuty	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptInvitation	Concede permissão para aceitar convites para se tornar uma conta de membro GuardDuty	Gravar			
ArchiveFindings	Concede permissão para arquivar GuardDuty descobertas	Gravar			
CreateDetector	Concede permissão para criar um detector	Gravar		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateFilter	Concede permissão para criar GuardDuty filtros. Um filtro define atributos e condições de descoberta usados para filtrar descobertas	Gravar	filter*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateIPSet	Concede permissão para criar um IPSet	Gravar		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	iam:DeleteRolePolicy iam:PutRolePolicy
CreateMalwareProtectionPlan	Concede permissão para criar um plano de proteção contra malware	Gravar		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateMembers	Concede permissão para criar contas de GuardDuty membros, em que a conta usada para criar um membro se torna a conta de GuardDuty administrador	Gravar			
CreatePublishingDestination	Concede permissão para criar um destino de publicação	Write			s3:GetObject s3:ListBucket

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSampleFindings	Concede permissão para criar exemplos de descobertas	Gravar			
CreateThreatEntitySet	Concede permissão para criar GuardDuty ThreatEntitySets, onde a ThreatEntitySet consiste em and/or domínios de endereços IP maliciosos conhecidos usados por GuardDuty para gerar descobertas	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
CreateThreatIntelSet	Concede permissão para criar GuardDuty ThreatIntelSets, onde a ThreatIntelSet consiste em endereços IP maliciosos conhecidos usados por GuardDuty para gerar descobertas	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTrustedEntitySet	Concede permissão para criar um TrustedEntitySet	Gravar		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeclineInvitations	Concede permissão para recusar convites para se tornar uma conta de membro GuardDuty	Gravar			
DeleteDetector	Concede permissão para excluir GuardDuty detectores	Gravar	detector*		
DeleteFilter	Concede permissão para excluir GuardDuty filtros	Gravar	filter*		
DeleteIPSet	Concede permissão para excluir GuardDuty IPSets	Gravar	ipset*		
DeleteInvitations	Concede permissão para excluir convites para se tornar uma conta de membro GuardDuty	Gravar			
DeleteMalwareProtectionPlan	Concede permissão para excluir um plano de proteção contra malware	Gravar	malwareprotectionplan*		
DeleteMembers	Concede permissão para excluir contas de GuardDuty membros	Gravar			
DeletePublishingDestination	Concede permissão para excluir um destino de publicação	Gravar	publishingDestination*		
DeleteThreatEntitySet	Concede permissão para excluir GuardDuty ThreatEntitySets	Gravar	threatentityset*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteThreatIntelSet	Concede permissão para excluir GuardDuty ThreatIntelSets	Gravar	threatintelset*		
DeleteTrustedEntitySet	Concede permissão para excluir GuardDuty TrustedEntitySets	Gravar	trustedentityset*		
DescribeMalwareScans	Concede permissão para recuperar detalhes sobre verificações de malware	Leitura			
DescribeOrganizationConfiguration	Concede permissão para recuperar detalhes sobre o administrador delegado associado a um detector GuardDuty	Leitura			
DescribePublishingDestination	Concede permissão para recuperar detalhes sobre um destino de publicação	Leitura	publishingDestination*		
DisableOrganizationAdminAccount	Concede permissão para desativar o administrador delegado da organização para GuardDuty	Gravar			
DisassociateFromAdministratorAccount	Concede permissão para desassociar uma conta de GuardDuty membro de sua conta de GuardDuty administrador	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateFromMasterAccount	Concede permissão para desassociar uma conta de GuardDuty membro de sua conta de GuardDuty administrador	Gravar			
DisassociateMembers	Concede permissão para desassociar contas de GuardDuty membros de sua conta de administrador GuardDuty	Gravar			
EnableOrganizationAdminAccount	Concede permissão para habilitar um administrador delegado da organização para GuardDuty	Gravar			
GetAdministratorAccount	Concede permissão para recuperar detalhes da conta de GuardDuty administrador associada a uma conta de membro	Leitura			
GetCoverageStatistics	Concede permissão para listar estatísticas de GuardDuty cobertura da Amazon para a GuardDuty conta especificada em uma região	Leitura	detector*		
GetDetector	Concede permissão para recuperar detectores GuardDuty	Leitura	detector*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetFilter	Concede permissão para recuperar filtros GuardDuty	Leitura	filter*		
GetFindings	Concede permissão para recuperar descobertas GuardDuty	Leitura			
GetFindingsStatistics	Concede permissão para recuperar uma lista de estatísticas de GuardDuty busca	Leitura			
GetIPSet	Concede permissão para recuperar GuardDuty IPSets	Leitura	ipset*		
GetInvitationsCount	Concede permissão para recuperar a contagem de todos os GuardDuty convites enviados para uma conta específica, que não inclui o convite aceito	Leitura			
GetMalwareProtectionPlan	Concede permissão para recuperar detalhes de um plano de proteção contra malware	Leitura	malwareprotectionplan*		
GetMalwareScanSettings	Concede permissão para recuperar as configurações de verificação de malware	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetMasterAccount	Concede permissão para recuperar detalhes da conta de GuardDuty administrador associada a uma conta de membro	Leitura			
GetMemberDetectors	Concede permissão para descrever quais fontes de dados estão habilitadas para detectores de contas de membro	Leitura			
GetMembers	Concede permissão para recuperar as contas-membro associadas a uma conta de administrador	Leitura			
GetOrganizationStatistics	Concede permissão para recuperar estatísticas de cobertura do plano de GuardDuty proteção para contas de membros em uma região	Leitura			
GetRemainingFreeTrialDays	Concede permissão para fornecer o número restante de dias para cada fonte de dados usada no período de teste gratuito	Leitura			
GetThreatEntitySet	Concede permissão para recuperar GuardDuty ThreatEntitySets	Leitura	threatentityset*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetThreatIntelSet	Concede permissão para recuperar GuardDuty ThreatIntelSets	Leitura	threatintelset*		
GetTrustedEntitySet	Concede permissão para recuperar GuardDuty TrustedEntitySets	Leitura	trustedentityset*		
GetUsageStatistics	Concede permissão para listar as estatísticas de GuardDuty uso da Amazon nos últimos 30 dias para o ID do detector especificado	Leitura			
InviteMembers	Concede permissão para convidar outras AWS contas para ativar GuardDuty e se tornar contas de GuardDuty membros	Gravar			
ListCoverage	Concede permissão para listar todos os detalhes de recursos de determinada conta na região	Lista	detector*		
ListDetectors	Concede permissão para recuperar uma lista de detectores GuardDuty	Lista			
ListFilters	Concede permissão para recuperar uma lista de filtros GuardDuty	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListFindings	Concede permissão para recuperar uma lista de descobertas GuardDuty	Lista			
ListIPSets	Concede permissão para recuperar uma lista de GuardDuty IPSets	Lista			
ListInvitations	Concede permissão para recuperar uma lista de todos os convites de GuardDuty associação que foram enviados para um Conta da AWS	Lista			
ListMalwareProtectionPlans	Concede permissão para recuperar uma lista de planos de proteção contra malware	Lista			
ListMembers	Concede permissão para recuperar uma lista de contas de GuardDuty membros associadas a uma conta de administrador	Lista			
ListOrganizationAdminAccounts	Concede permissão para listar detalhes sobre o administrador delegado da organização para GuardDuty	Lista			
ListPublishingDestinations	Concede permissão para recuperar uma lista de destinos de publicação	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para recuperar uma lista de tags associadas a um recurso GuardDuty	Leitura	detector		
			filter		
			ipset		
			malwareprotectionplan		
			threatentityset		
			threatintelset		
			trustedentityset		
ListThreatEntitySets	Concede permissão para recuperar uma lista de GuardDuty ThreatEntitySets	Lista			
ListThreatIntelSets	Concede permissão para recuperar uma lista de GuardDuty ThreatIntelSets	Lista			
ListTrustedEntitySets	Concede permissão para recuperar uma lista de GuardDuty TrustedEntitySets	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SendSecurityTelemetry	Concede permissão para enviar telemetria de segurança para uma GuardDuty conta específica em uma região	Gravar			
StartMalwareScan	Concede permissão para iniciar uma nova verificação de malware	Gravar			
StartMonitoringMembers	Concede permissão a uma conta de GuardDuty administrador para monitorar as descobertas das contas GuardDuty dos membros	Gravar			
StopMonitoringMembers	Concede permissão para desabilitar o monitoramento de descobertas das contas-membro	Gravar			
TagResource	Concede permissão para adicionar tags a um GuardDuty recurso	Tags	detector		
			filter		
			ipset		
			malwareprotectionplan		
			threatintelset		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			threatintelset		
			trustedentityset		
				aws:RequestTag/${TagKey} aws:TagKeys	
Unarchive Findings	Concede permissão para desarquivar descobertas GuardDuty	Gravar			
UntagResource	Concede permissão para remover tags de um GuardDuty recurso	Tags	detector		
			filter		
			ipset		
			malwareprotectionplan		
			threatentityset		
			threatintelset		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			trustedentityset		
				aws:TagKeys	
UpdateDetector	Concede permissão para atualizar GuardDuty detectores	Gravar	detector*		
UpdateFilter	Concede permissão para atualizar GuardDuty filtros	Gravar	filter*		
UpdateFindingsFeedback	Concede permissão para atualizar as descobertas. Feedback para marcar as GuardDuty descobertas como úteis ou não úteis	Gravar			
UpdateIPSet	Concede permissão para atualizar GuardDuty IPSets	Gravar	ipset*		iam:DeleteRolePolicy iam:PutRolePolicy
UpdateMalwareProtectionPlan	Concede permissão para atualizar o plano de proteção contra malware	Gravar	malwareprotectionplan*		
UpdateMalwareScanSettings	Concede permissão para atualizar as configurações de verificação de malware	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateMemberDetectors	Concede permissão para atualizar quais fontes de dados estão habilitadas para detectores de contas de membro	Gravar			
UpdateOrganizationConfiguration	Concede permissão para atualizar a configuração do administrador delegado associada a um detector GuardDuty	Gravar			
UpdatePublishingDestination	Concede permissão para atualizar um destino de publicação	Gravar	publishingDestination*		s3:GetObject s3:ListBucket
UpdateThreatEntitySet	Concede permissão para atualizar GuardDuty ThreatEntitySets	Gravar	threatentityset*		s3:GetObject
UpdateThreatIntelSet	Concede permissão para atualizar o GuardDuty ThreatIntelSets	Gravar	threatintelset*		iam:DeleteRolePolicy iam:PutRolePolicy
UpdateTrustedEntitySet	Concede permissão para atualizar GuardDuty TrustedEntitySets	Gravar	trustedentityset*		s3:GetObject

Tipos de recursos definidos pela Amazon GuardDuty

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
detector	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}`	aws:ResourceTag/${TagKey}
filter	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/filter/${FilterName}`	aws:ResourceTag/${TagKey}
ipset	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/ipset/${IPSetId}`	aws:ResourceTag/${TagKey}
threatintelset	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/threatintelset/${ThreatIntelSetId}`	aws:ResourceTag/${TagKey}
trustedentityset	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/trustedentityset/${TrustedEntitySetId}`	aws:ResourceTag/${TagKey}
threatentityset	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/threatentityset/${ThreatEntitySetId}`	aws:ResourceTag/${TagKey}
publishingDestination	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/p`	

Tipos de recursos	ARN	Chaves de condição
	`ublishingDestination/${PublishingDestinationId}`	
malwareprotectionplan	`arn:${Partition}:guardduty:${Region}:${Account}:malware-protection-plan/${MalwareProtectionPlanId}`	aws:ResourceTag/${TagKey}

Chaves de condição para a Amazon GuardDuty

A Amazon GuardDuty define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para AWS Health APIs and Notifications

AWS Health APIs and Notifications (prefixo do serviço:`health`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas por AWS Health APIs and Notifications
- Tipos de recursos definidos por AWS Health APIs and Notifications
- Chaves de condição para AWS Health APIs and Notifications

Ações definidas por AWS Health APIs and Notifications

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar

a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeAffectedAccountsForOrganization	Concede permissão para recuperar uma lista de contas que foram afetadas pelos eventos especificados na organização	Leitura			organizations:ListAccounts
DescribeAffectedEntities	Concede permissão para recuperar uma lista de entidades que foram afetadas pelos eventos especificados	Leitura	event*		
				health:eventTypeCode	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				health:service	
DescribeAffectedEntitiesForOrganization	Concede permissão para recuperar uma lista de entidades que foram afetadas pelos eventos e pelas contas especificados na organização	Leitura			organizations:ListAccounts
DescribeEntityAggregates	Concede permissão para recuperar o número de entidades afetadas por cada um dos eventos especificados	Leitura			
DescribeEntityAggregatesForOrganization	Concede permissão para recuperar o número de entidades afetadas por cada um dos eventos especificados em uma organização	Leitura			organizations:ListAccounts
DescribeEventAggregates	Concede permissão para recuperar o número de eventos de cada tipo de evento (problema, alteração programada e notificação de conta)	Leitura			
DescribeEventDetails	Concede permissão para recuperar informações detalhadas sobre um ou mais eventos especificados	Leitura	event*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				health:eventTypeCode health:service	
DescribeEventDetailsForOrganization	Concede permissão para recuperar informações detalhadas sobre um ou mais eventos especificados para contas fornecidas na organização	Leitura			organizations:ListAccounts
DescribeEventTypes	Concede permissão para recuperar os tipos de eventos que atendem aos critérios de filtro especificados	Leitura			
DescribeEvents	Concede permissão para recuperar informações sobre um ou mais eventos que correspondem aos critérios de filtro especificados	Leitura			
DescribeEventsForOrganization	Concede permissão para recuperar informações sobre um ou mais eventos que atendem aos critérios de filtro especificados na organização	Leitura			organizations:ListAccounts

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeHealthServiceStatusForOrganization	Concede permissão para recuperar o status de habilitação ou desabilitação do recurso de visualização organizacional	Leitura			organizations:ListAccounts
DisableHealthServiceAccessForOrganization	Concede permissão para desabilitar o recurso de visualização organizacional	Gerenciamento de permissões			organizations:DisableAWSServiceAccess organizations:ListAccounts
EnableHealthServiceAccessForOrganization	Concede permissão para habilitar o recurso de visualização organizacional	Gerenciamento de permissões			iam:CreateServiceLinkedRole organizations:EnableAWSServiceAccess organizations:ListAccounts

Tipos de recursos definidos por AWS Health APIs and Notifications

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações

identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
event	`arn:${Partition}:health:*::event/${Service}/${EventTypeCode}/*`	

Chaves de condição para AWS Health APIs and Notifications

AWS Health APIs and Notifications define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
health:eventTypeCode	Filtra o acesso por tipo de evento	String
health:service	Filtra o acesso por serviço afetado	String

Ações, recursos e chaves de condição para o AWS HealthImaging

AWS HealthImaging (prefixo do serviço:`medical-imaging`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.

- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS HealthImaging
- Tipos de recursos definidos pelo AWS HealthImaging
- Chaves de condição do AWS HealthImaging

Ações definidas pelo AWS HealthImaging

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CopyImageSet	Concede permissão para copiar um conjunto de imagens	Gravar	datastore*		
			imageset*		
CreateDatastore	Concede permissão para criar um armazenamento de dados para ingerir dados de imagem	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDatastore	Concede permissão para excluir um armazenamento de dados	Gravar	datastore*		
DeleteImageSet	Concede permissão para excluir um conjunto de imagens	Gravar	datastore*		
			imageset*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetDICOMBulkdata	Concede permissão para obter dados em massa dicom em formato binário	Leitura	datastore*		
GetDICOMImportJob	Concede permissão para obter as propriedades de um trabalho de importação	Leitura	datastore*		
GetDICOMInstance	Concede permissão para obter uma instância DICOM no formato DCM	Leitura	datastore*		
GetDICOMInstanceFrames	Concede permissão para obter quadros de instância DICOM no formato solicitado pelo cliente	Leitura	datastore*		
GetDICOMInstanceMetadata	Concede permissão para obter metadados de instância DICOM no formato DICOM JSON	Leitura	datastore*		
GetDICOMSeriesMetadata	Concede permissão para recuperar metadados para todas as instâncias DICOM pertencentes a uma determinada série DICOM no formato DICOM JSON	Leitura	datastore*		
GetDatastore	Concede permissão para obter propriedades do armazenamento de dados	Leitura	datastore*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetImageFrame	Concede permissão para obter propriedades do quadro de imagem	Leitura	datastore*		
			imageset*		
GetImageSet	Concede permissão para obter propriedades do conjunto de imagens	Leitura	datastore*		
			imageset*		
GetImageSetMetadata	Concede permissão para obter propriedades de metadados do conjunto de imagens	Leitura	datastore*		
			imageset*		
ListDICOMImportJobs	Concede permissão para listar trabalhos de importação para um armazenamento de dados	Lista	datastore*		
ListDatastores	Concede permissão para listar armazenamentos de dados	Lista			
ListImageSetVersions	Concede permissão para listar versões de um conjunto de imagens	Lista	datastore*		
			imageset*		
ListTagsForResource	Concede permissão para listar tags para um recurso de imagens médicas	Lista	datastore		
			imageset		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SearchDICOMInstances	Concede permissão para pesquisar instâncias dicom que retornam dados no formato DICOM JSON	Leitura	datastore*		
SearchDICOMSeries	Concede permissão para pesquisar séries dicom que retornam dados no formato DICOM JSON	Leitura	datastore*		
SearchDICOMStudies	Concede permissão para pesquisar estudos dicom que retornam dados no formato DICOM JSON	Leitura	datastore*		
SearchImageSets	Concede permissão para pesquisar conjuntos de imagens	Leitura	datastore*		
StartDICOMImportJob	Concede permissão para iniciar um trabalho de importação DICOM	Gravar	datastore*		
StoreDICOM	Concede permissão para armazenar instâncias dicom que retornam o resultado no formato DICOM JSON	Gravar	datastore*		
StoreDICOMStudy	Concede permissão para armazenar um estudo dicom que retorna o resultado no formato DICOM JSON	Gravar	datastore*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para adicionar tags a um recurso de imagens médicas	Tags	datastore		
			imageset		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover tags de um recurso de imagens médicas	Tags	datastore		
			imageset		
				aws:TagKeys	
UpdateImageSetMetadata	Concede permissão para atualizar as propriedades de metadados do conjunto de imagens	Gravar	datastore*		
			imageset*		

Tipos de recursos definidos pelo AWS HealthImaging

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves

são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS HealthImaging

AWS HealthImaging define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por um par de chave valor da etiqueta que é permitido na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso por um par de chave e valor da etiqueta de um recurso.	Segmento
aws:TagKeys	Filtra o acesso por uma lista de chaves da etiqueta que são permitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS HealthLake

AWS HealthLake (prefixo do serviço:`healthlake`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS HealthLake
- Tipos de recursos definidos pelo AWS HealthLake
- Chaves de condição do AWS HealthLake

Ações definidas pelo AWS HealthLake

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelFHIRExportJobWithDelete	Concede permissão para cancelar um trabalho de exportação FHIR em andamento com Delete	Gravar	datastore*		
CreateFHIRDatastore	Concede permissão para criar um datastore que possa ingerir e exportar dados FHIR	Gravação		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateResource	Concede permissão para criar um recurso	Gravação	datastore*		
DeleteFHIRDatastore	Concede permissão para excluir um datastore	Gravação	datastore*		
DeleteResource	Concede permissão para excluir um recurso	Gravação	datastore*		
DescribeFHIRDatastore	Concede permissão para obter as propriedades associadas ao datastore FHIR, incluindo o ID, o ARN, o nome, o status, a data de criação, a versão do tipo e o endpoint do datastore	Leitura	datastore*		
DescribeFHIRExportJob	Concede permissão para exibir as propriedades de um trabalho de exportação FHIR, incluindo o ID, o ARN, o nome e o status do datastore	Leitura	datastore*		
DescribeFHIRExportJobWithGet	Concede permissão para exibir as propriedades de um trabalho de exportação FHIR, incluindo o ID, o ARN, o nome e o status do datastore com Get	Leitura	datastore*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeFHIRImportJob	Concede permissão para exibir as propriedades de um trabalho de importação FHIR, incluindo o ID, ARN, nome e o status do datastore	Leitura	datastore*		
GetCapabilities	Concede permissão para obter os recursos de um datastore FHIR	Leitura	datastore*		
GetExportedFile	Concede permissão para acessar arquivos exportados de um trabalho de exportação FHIR iniciado com Get	Leitura	datastore*		
GetHistoryByResourceId	Concede permissão para ler o histórico de recursos	Leitura	datastore*		
ListFHIRDatastores	Concede permissão para listar todos os datastores FHIR que estão na conta do usuário, independentemente do status do datastore	Lista			
ListFHIRExportJobs	Concede permissão para obter uma lista de trabalhos de exportação para o datastore especificado	List	datastore*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListFHIRImportJobs	Concede permissão para obter uma lista de trabalhos de importação para o datastore especificado	List	datastore*		
ListTagsForResource	Concede permissão para obter uma lista de etiquetas para o datastore especificado	Lista	datastore		
ProcessBundle	Concede permissão para agrupar várias operações de recursos	Gravar	datastore*		
ReadResource	Concede permissão para ler um recurso	Leitura	datastore*		
SearchEverything	Concede permissão para pesquisar todos os recursos relacionados a um paciente	Leitura	datastore*		
SearchWithGet	Concede permissão para pesquisar recursos com o método GET	Leitura	datastore*		
SearchWithPost	Concede permissão para pesquisar recursos com o método POST	Leitura	datastore*		
StartFHIRExportJob	Concede permissão para iniciar um trabalho de exportação FHIR	Gravar	datastore*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartFHIRExportJobWithGet	Concede permissão para iniciar um trabalho de exportação FHIR com Get	Gravar	datastore*		
StartFHIRExportJobWithPost	Concede permissão para iniciar um trabalho de exportação FHIR com o Post	Gravar	datastore*		
StartFHIRImportJob	Concede permissão para iniciar um trabalho de importação FHIR	Gravação	datastore*		
TagResource	Concede permissão para adicionar etiquetas a um datastore	Marcação	datastore		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permissão para remover etiquetas associadas a um datastore	Marcação	datastore		
				aws:TagKeys	
UpdateResource	Concede permissão para atualizar um recurso	Gravar	datastore*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
VersionReadResource	Concede permissão para ler a versão de um recurso	Leitura	datastore *		

Tipos de recursos definidos pelo AWS HealthLake

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
datastore	`arn:${Partition}:healthlake:${Region}:${Account}:datastore/fhir/${DatastoreId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS HealthLake

AWS HealthLake define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pela presença de pares chave-valor da etiqueta anexados ao recurso	Segmento
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS HealthOmics

AWS HealthOmics (prefixo do serviço:`omics`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS HealthOmics
- Tipos de recursos definidos pelo AWS HealthOmics
- Chaves de condição do AWS HealthOmics

Ações definidas pelo AWS HealthOmics

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AbortMultipartReadSetUpload	Concede permissão para anular uploads de conjuntos de leitura fracionados	Gravar	sequenceStore*		
AcceptShare	Concede permissão para aceitar um compartilhamento	Gravar			
BatchDeleteReadSet	Concede permissão para excluir conjuntos de leitura em lote em um determinado armazenamento de sequências	Gravar	sequenceStore*		
CancelAnnotationImportJob	Concede permissão para cancelar um trabalho de importação de anotações	Gravar			
CancelRun	Concede permissão para cancelar a execução de um fluxo de trabalho e interromper todas as tarefas de fluxo de trabalho	Gravar	run*		
CancelVariantImportJob	Concede permissão para cancelar um trabalho de importação de variantes	Gravar			
CompleteMultipartReadSetUpload	Concede permissão para concluir um upload de conjunto de leitura fracionado	Gravar	sequenceStore*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAnnotationStore	Concede permissão para criar um armazenamento de anotações	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAnnotationStoreVersion	Concede permissão para criar uma versão em um armazenamento de anotações	Gravar	AnnotationStore*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMultipartReadSetUpload	Concede permissão para criar um upload de conjunto de leitura fracionado	Gravar	sequenceStore*		
CreateReferenceStore	Concede permissão para criar um armazenamento de referência	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRunCache	Concede permissão para criar um novo cache de execução do fluxo de trabalho	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateRunGroup	Concede permissão para criar um novo grupo de execução de fluxo de trabalho	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSequenceStore	Concede permissão para criar um armazenamento de sequências	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateShare	Concede permissão para criar um compartilhamento	Gravar			
CreateVariantStore	Concede permissão para criar um armazenamento de variantes	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkflow	Concede permissão para criar um novo fluxo de trabalho com uma definição de fluxo de trabalho e um modelo de parâmetros de fluxos de trabalho	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateWorkflowVersion	Concede permissão para criar uma nova versão do fluxo de trabalho com uma definição de fluxo de trabalho e um modelo de parâmetros do fluxo de trabalho	Gravar	workflow*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAnnotationStore	Concede permissão para excluir um armazenamento de anotações	Gravar	AnnotationStore*		
DeleteAnnotationStoreVersions	Concede permissão para excluir versões em um armazenamento de anotações	Gravar	AnnotationStore*		
			AnnotationStoreVersion*		
DeleteReference	Concede permissão para excluir uma referência em um determinado armazenamento de referências	Gravar	reference*		
			referenceStore*		
DeleteReferenceStore	Concede permissão para excluir um armazenamento de referências	Gravar	referenceStore*		
DeleteRun	Concede permissão para excluir uma execução de fluxo de trabalho	Gravar	run*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteRunCache	Concede permissão para excluir um cache de execução do fluxo de trabalho	Gravar	runCache*		
DeleteRunGroup	Concede permissão para excluir um grupo de execução de fluxo de trabalho	Gravar	runGroup*		
DeleteS3AccessPolicy	Concede permissão para excluir uma política de acesso em uma determinada loja	Gravar	sequenceStore*		
DeleteSequenceStore	Concede permissão para excluir um armazenamento de sequências	Gravar	sequenceStore*		
DeleteShare	Concede permissão para excluir um compartilhamento	Gravar			
DeleteVariantStore	Concede permissão para excluir um armazenamento de variantes	Gravar	VariantStore*		
DeleteWorkflow	Concede permissão para excluir um fluxo de trabalho	Gravar	workflow*		
DeleteWorkflowVersion	Concede permissão para excluir uma versão do fluxo de trabalho	Gravar	WorkflowVersion*		
			workflow*		
GetAnnotationImportJob	Concede permissão para obter o status de um trabalho de importação de anotações	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAnnotationStore	Concede permissão para obter informações detalhadas sobre um armazenamento de anotações	Leitura	AnnotationStore*		
GetAnnotationStoreVersion	Concede permissão para obter informações detalhadas sobre uma versão em um armazenamento de anotações	Leitura	AnnotationStoreVersion*		
GetReadSet	Concede permissão para obter um conjunto de leitura em um determinado armazenamento de sequências	Leitura	readSet* sequenceStore*		
GetReadSetActivationJob	Concede permissão para obter detalhes sobre um trabalho de ativação de conjunto de leitura em um determinado armazenamento de sequências	Leitura	sequenceStore*		
GetReadSetExportJob	Concede permissão para obter detalhes sobre um trabalho de exportação de conjunto de leitura em um determinado armazenamento de sequências	Leitura	sequenceStore*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetReadSetImportJob	Concede permissão para obter detalhes sobre um trabalho de importação de conjunto de leitura em um determinado armazenamento de sequências	Leitura	sequenceStore*		
GetReadSetMetadata	Concede permissão para obter detalhes sobre um conjunto de leitura em um determinado armazenamento de sequências	Leitura	readSet*		
			sequenceStore*		
GetReference	Concede permissão para obter uma referência em um determinado armazenamento de referências	Leitura	reference*		
			referenceStore*		
GetReferenceImportJob	Concede permissão para obter detalhes sobre um trabalho de importação de referências em um determinado armazenamento de referências	Leitura	referenceStore*		
GetReferenceMetadata	Concede permissão para obter detalhes sobre uma referência em um determinado armazenamento de referências	Leitura	reference*		
			referenceStore*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetReferenceStore	Concede permissão para obter detalhes sobre um armazenamento de referências	Leitura	referenceStore*		
GetRun	Concede permissão para recuperar detalhes de uma execução de fluxo de trabalho	Leitura	run*		
GetRunCache	Concede permissão para recuperar detalhes do cache de execução do fluxo de trabalho	Leitura	runCache*		
GetRunGroup	Concede permissão para recuperar detalhes de um grupo de execução de fluxo de trabalho	Leitura	runGroup*		
GetRunTask	Concede permissão para recuperar detalhes de uma tarefa de fluxo de trabalho	Leitura	TaskResource* run*		
GetS3AccessPolicy	Concede permissão para obter detalhes sobre uma política de acesso em uma determinada loja	Leitura	sequenceStore*		
GetSequenceStore	Concede permissão para obter detalhes sobre um armazenamento de sequências	Leitura	sequenceStore*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetShare	Concede permissão para obter informações detalhadas sobre um compartilhamento	Leitura			
GetVariantImportJob	Concede permissão para obter o status de um trabalho de importação de variantes	Leitura			
GetVariantStore	Concede permissão para obter informações detalhadas sobre um armazenamento de variantes	Leitura	VariantStore*		
GetWorkflow	Concede permissão para recuperar detalhes de um fluxo de trabalho	Leitura	workflow*		
GetWorkflowVersion	Concede permissão para recuperar detalhes da versão do fluxo de trabalho	Leitura	WorkflowVersion* workflow*		
ListAnnotationImportJobs	Concede permissão para obter uma lista de trabalhos de importação de anotações	Lista			
ListAnnotationStoreVersions	Concede permissão para recuperar uma lista de informações sobre versões em um repositório de anotações	Lista	AnnotationStore*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAnnotationStores	Concede permissão para recuperar uma lista de informações sobre repositórios de anotações	Lista			
ListMultipartReadSetUploads	Concede permissão para listar uploads de conjuntos de leitura fracionados	Lista	sequenceStore*		
ListReadSetActivationJobs	Concede permissão para listar trabalhos de ativação de conjunto de leitura em um determinado armazenamento de sequências	Lista	sequenceStore*		
ListReadSetExportJobs	Concede permissão para listar trabalhos de exportação de conjunto de leitura em um determinado armazenamento de sequências	Lista	sequenceStore*		
ListReadSetImportJobs	Concede permissão para listar trabalhos de importação de conjunto de leitura em um determinado armazenamento de sequências	Lista	sequenceStore*		
ListReadSetUploadParts	Concede permissão para listar partes de uploads de conjuntos de leitura	Lista	sequenceStore*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListReadSets	Concede permissão para listar conjuntos de leitura em um determinado armazenamento de sequências	Lista	sequenceStore*		
ListReferenceImportJobs	Concede permissão para listar trabalhos de importação de referências em um determinado armazenamento de referências	Lista	referenceStore*		
ListReferenceStores	Concede permissão para listar armazenamentos de referências	Lista			
ListReferences	Concede permissão para listar referências em um determinado armazenamento de referências	Lista	referenceStore*		
ListRunCaches	Concede permissão para recuperar uma lista de caches de execução do fluxo de trabalho	Lista			
ListRunGroups	Concede permissão para recuperar uma lista de grupos de execução de fluxos de trabalho	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListRunTasks	Concede permissão para recuperar uma lista de tarefas da uma execução de fluxo de trabalho	Lista	run*		
ListRuns	Concede permissão para recuperar uma lista de execuções de fluxos de trabalho	Lista			
ListSequenceStores	Concede permissão para listar armazenamentos de sequências	Lista			
ListShares	Concede permissão para recuperar uma lista de informações sobre compartilhamentos	Lista			
ListTagsForResource	Concede permissão para recuperar uma lista de tags de recursos AWS	Lista			
ListVariantImportJobs	Concede permissão para obter uma lista de trabalhos de importação de variantes	Lista			
ListVariantStores	Concede permissão para recuperar uma lista de metadados para armazenamentos de variantes	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListWorkflowVersions	Concede permissão para recuperar uma lista das versões disponíveis para um fluxo de trabalho	Lista	workflow*		
ListWorkflows	Concede permissão para recuperar uma lista de fluxos de trabalho disponíveis	Lista			
PutS3AccessPolicy	Concede permissão para colocar uma política de acesso em uma determinada loja	Gravar	sequenceStore*		
StartAnnotationImportJob	Concede permissão para importar uma lista de arquivos de anotação para um armazenamento de anotações	Gravar	AnnotationStore* AnnotationStoreVersion*		
StartReadSetActivationJob	Concede permissão para iniciar um trabalho de ativação de conjunto de leitura de um determinado armazenamento de sequências	Gravar	sequenceStore*		
StartReadSetExportJob	Concede permissão para iniciar um trabalho de exportação de conjunto de leitura de um determinado armazenamento de sequências	Gravar	sequenceStore*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartReadSetImportJob	Concede permissão para iniciar um trabalho de importação de conjunto de leitura em um determinado armazenamento de sequências	Gravar	sequenceStore*		
StartReferenceImportJob	Concede permissão para iniciar um trabalho de importação de referências em um determinado armazenamento de referências	Gravar	referenceStore*		
StartRun	Concede permissão para iniciar a execução de um fluxo de trabalho	Gravar	run*		iam:PassRole
			runCache		
			runGroup		
			workflow		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartVariantImportJob	Concede permissão para importar uma lista de arquivos de variantes para um armazenamento de variantes	Gravar	VariantStore*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para adicionar AWS tags a um recurso	Tags	AnnotationStore		
			AnnotationStoreVersion		
			VariantStore		
			WorkflowVersion		
			readSet		
			reference		
			referenceStore		
			run		
			runCache		
			runGroup		
			sequenceStore		
			workflow		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover AWS tags de recursos	Tags	AnnotationStore		
			AnnotationStoreVersion		
			VariantStore		
			WorkflowVersion		
			readSet		
			reference		
			referenceStore		
			run		
			runCache		
			runGroup		
			sequenceStore		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			workflow		
				aws:TagKeys	
UpdateAnnotationStore	Concede permissão para atualizar informações sobre o armazenamento de anotações	Gravar	AnnotationStore*		
UpdateAnnotationStoreVersion	Concede permissão para atualizar informações sobre a versão em um armazenamento de anotações	Gravar	AnnotationStoreVersion*		
UpdateRunCache	Concede permissão para atualizar um cache de execução do fluxo de trabalho	Gravar	runCache*		
UpdateRunGroup	Concede permissão para atualizar um grupo de execução de fluxo de trabalho	Gravar	runGroup*		
UpdateSequenceStore	Concede permissão para atualizar detalhes sobre um Sequence Store	Gravar	sequenceStore*		
UpdateVariantStore	Concede permissão para atualizar os metadados sobre o armazenamento de variantes	Gravar	VariantStore*		
UpdateWorkflow	Concede permissão para atualizar detalhes de um fluxo de trabalho	Gravar	workflow*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateWorkflowVersion	Concede permissão para atualizar os detalhes da versão do fluxo de trabalho	Gravar	WorkflowVersion*		
			workflow*		
UploadReadSetPart	Concede permissão para fazer upload de partes do conjunto de leitura	Gravar	sequenceStore*		

Tipos de recursos definidos pelo AWS HealthOmics

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
AnnotationStore	`arn:${Partition}:omics:${Region}:${Account}:annotationStore/${AnnotationStoreName}`	aws:ResourceTag/${TagKey}
AnnotationStoreVersion	`arn:${Partition}:omics:${Region}:${Account}:annotationStore/${AnnotationStoreName}/version/${AnnotationStoreVersionName}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
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/${TagKey}
TaggingResource	arn:${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}

Tipos de recursos	ARN	Chaves de condição
workflow	`arn:${Partition}:omics:${Region}:${Account}:workflow/${Id}`	aws:ResourceTag/${TagKey}
WorkflowVersion	`arn:${Partition}:omics:${Region}:${Account}:workflow/${Id}/version/${VersionName}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS HealthOmics

AWS HealthOmics define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pela presença de pares chave-valor da etiqueta anexados ao recurso	Segmento
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Honeycode

O Amazon Honeycode (prefixo do serviço: `honeycode`) fornece os recursos, as ações e as chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Honeycode
- Tipos de recursos definidos pelo Amazon Honeycode
- Chaves de condição do Amazon Honeycode

Ações definidas pelo Amazon Honeycode

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ApproveTeamAssociation [somente permissão]	Concede permissão para aprovar uma solicitação de associação de equipe para sua Conta AWS	Gravar			
BatchCreateTableRows	Concede permissão para criar novas linhas em uma tabela	Write	table*		
BatchDeleteTableRows	Concede permissão para excluir linhas de uma tabela	Write	table*		
BatchUpdateTableRows	Concede permissão para atualizar linhas em uma tabela	Write	table*		
BatchUpsertTableRows	Concede permissão para inserir linhas em uma tabela	Write	table*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateTeam [somente permissão]	Concede permissão para criar uma nova equipe Amazon Honeycode para sua conta AWS	Gravar			
CreateTenant [somente permissão]	Concede permissão para criar um novo inquilino no Amazon Honeycode para sua conta AWS	Gravar			
DeleteDomains [somente permissão]	Concede permissão para excluir domínios Amazon Honeycode para sua conta AWS	Gravar			
DeregisterGroups [somente permissão]	Concede permissão para remover grupos de uma equipe do Amazon Honeycode para sua conta AWS	Gravar			
DescribeTableDataImportJob	Concede permissão para obter detalhes sobre um trabalho de importação de dados de tabela	Read	table*		
DescribeTeam [somente permissão]	Concede permissão para obter detalhes sobre as equipes do Amazon Honeycode para sua conta AWS	Leitura			
GetScreenData	Concede permissão para carregar os dados de uma tela	Read	screen*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
InvokeScreenAutomation	Concede permissão para invocar uma automação de tela	Write	screen-automation*		
ListDomains [somente permissão]	Concede permissão para listar todos os domínios do Amazon Honeycode e seu status de verificação para sua conta AWS	Lista			
ListGroups [somente permissão]	Concede permissão para listar todos os grupos em uma equipe Amazon Honeycode para sua conta AWS	Lista			
ListTableColumns	Concede permissão para listar as colunas em uma tabela	List	table*		
ListTableRows	Concede permissão para listar as linhas em uma tabela	List	table*		
ListTables	Concede permissão para listar as tabelas em uma pasta de trabalho	Lista	workbook*		
ListTagsForResource	Concede permissão para listar todas as etiquetas de um recurso	Tags			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTeamAssociations [somente permissão]	Concede permissão para listar todas as associações de equipe pendentes e aprovadas com sua AWS conta	Lista			
ListTenants [somente permissão]	Concede permissão para listar todos os inquilinos do Amazon Honeycode para sua conta AWS	Lista			
QueryTableRows	Concede permissão para consultar as linhas de uma tabela usando um filtro	Read	table*		
RegisterDomainForVerification [somente permissão]	Concede permissão para solicitar a verificação dos domínios Amazon Honeycode para sua conta AWS	Gravar			
RegisterGroups [somente permissão]	Concede permissão para adicionar grupos a uma equipe do Amazon Honeycode para sua conta AWS	Gravar			
RejectTeamAssociation [somente permissão]	Concede permissão para rejeitar uma solicitação de associação de equipe para sua AWS Conta	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RestartDomainVerification [somente permissão]	Concede permissão para reiniciar a verificação dos domínios Amazon Honeycode para sua conta AWS	Gravar			
StartTableDataImportJob	Concede permissão para iniciar um trabalho de importação de dados de tabela	Gravar	table*		
TagResource	Concede permissão para marcar um recurso	Marcação			
UntagResource	Concede permissão para desmarcar um recurso	Marcação			
UpdateTeam [somente permissão]	Concede permissão para atualizar uma equipe do Amazon Honeycode para sua conta AWS	Gravar			

Tipos de recursos definidos pelo Amazon Honeycode

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}`	

Chaves de condição do Amazon Honeycode

O Honeycode não tem chaves de contexto específicas do serviço que podem ser usadas no elemento `Condition` de instruções da política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS IAM Access Analyzer

AWS O IAM Access Analyzer (prefixo do serviço:`access-analyzer`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.

- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS IAM Access Analyzer
- Tipos de recursos definidos pelo AWS IAM Access Analyzer
- Chaves de condição do AWS IAM Access Analyzer

Ações definidas pelo AWS IAM Access Analyzer

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ApplyArchiveRule	Concede permissão para aplicar uma regra de arquivamento	Write	Analyzer*		
CancelPolicyGeneration	Concede permissão para cancelar uma geração de política	Gravar			
CheckAccessNotGranted	Concede permissão para verificar se o acesso especificado não é permitido por uma política	Leitura			
CheckNoNewAccess	Concede permissão para verificar se nenhum novo acesso é permitido quando comparado a uma política existente	Leitura			
CheckNoPublicAccess	Concede permissão para verificar se o acesso público	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	não é permitido por uma política de recursos				
CreateAccessPreview	Concede permissão para criar uma visualização de acesso para o analisador especificado	Write	Analyzer*		
CreateAnalyzer	Concede permissão para criar um analisador	Write	Analyzer*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateArchiveRule	Concede permissão para criar uma regra de arquivamento para o analisador especificado	Write	ArchiveRule*		
DeleteAnalyzer	Concede permissão para excluir o analisador especificado	Write	Analyzer*		
DeleteArchiveRule	Concede permissão para excluir regras de arquivamento para o analisador especificado	Gravar	ArchiveRule*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GenerateFindingRecommendation	Concede permissão para gerar etapas de recomendação para resolver uma descoberta	Gravar	Analyzer*		
GetAccessPreview	Concede permissão para recuperar informações sobre uma visualização de acesso	Read	Analyzer*		
GetAnalyzedResource	Concede permissão para recuperar informações sobre um recurso analisado	Read	Analyzer*		
GetAnalyzer	Concede permissão para recuperar informações sobre analisadores	Read	Analyzer*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetArchiveRule	Concede permissão para recuperar informações sobre regras de arquivamento para o analisador especificado	Read	ArchiveRule*		
GetFinding	Concede permissão para recuperar descobertas	Leitura	Analyzer*		
GetFindingRecommendation	Concede permissão para recuperar as etapas de recomendação para resolver uma descoberta	Leitura	Analyzer*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetFindingsStatistics	Concede permissão para recuperar estatísticas de descobertas	Leitura	Analyzer*		
GetGeneratedPolicy	Concede permissão para recuperar uma política que foi gerada usando StartPolicyGeneration	Leitura			
ListAccessPreviewFindings	Concede permissão para recuperar uma lista de descobertas de uma visualização de acesso	Read	Analyzer*		
ListAccessPreviews	Concede permissão para recuperar uma lista de visualizações de acesso	List	Analyzer*		
ListAnalyzedResources	Concede permissão para recuperar uma lista de recursos que foram analisados	Read	Analyzer*		
ListAnalyzers	Concede permissão para recuperar uma lista de analisadores	List			
ListArchiveRules	Concede permissão para recuperar uma lista de regras de arquivamento de um analisador	List	Analyzer*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListFindings	Concede permissão para recuperar uma lista de descobertas de um analisador	Read	Analyzer*		
ListPolicyGenerations	Concede permissão para listar todas as gerações de políticas iniciadas recentemente	Read			
ListTagsForResource	Concede permissão para recuperar uma lista de etiquetas aplicadas a um recurso	Read	Analyzer		
StartPolicyGeneration	Concede permissão para iniciar uma geração de políticas	Write			iam:PassRole
StartResourceScan	Concede permissão para iniciar uma verificação das políticas aplicadas a um recurso	Write	Analyzer*		
TagResource	Concede permissão para adicionar uma etiqueta a um recurso	Marcação	Analyzer		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover uma etiqueta de um recurso	Tags	Analyzer		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
UpdateAnalyzer	Concede permissão para modificar a configuração de um analisador	Gravar	Analyzer*		
UpdateArchiveRule	Concede permissão para modificar uma regra de arquivamento	Write	ArchiveRule*		
UpdateFindings	Concede permissão para modificar descobertas	Write	Analyzer*		
ValidatePolicy	Concede permissão para validar uma política	Read			

Tipos de recursos definidos pelo AWS IAM Access Analyzer

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
Analyzer	`arn:${Partition}:access-analyzer:${Region}:${Account}:analyzer/${AnalyzerName}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
ArchiveRule	`arn:${Partition}:access-analyzer:${Region}:${Account}:analyzer/${AnalyzerName}/archive-rule/${RuleName}`	

Chaves de condição do AWS IAM Access Analyzer

AWS O IAM Access Analyzer define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base na presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra ações com base nos pares de chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações com base na presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS IAM Identity Center

AWS O IAM Identity Center (prefixo do serviço:`sso`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS IAM Identity Center
- Tipos de recursos definidos pelo AWS IAM Identity Center
- Chaves de condição para o AWS IAM Identity Center

Ações definidas pelo AWS IAM Identity Center

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de

condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateDirectory	Concede permissão para conectar um diretório a ser usado pelo AWS IAM Identity Center	Gravar			ds:AuthorizeApplication
AssociateProfile	Concede permissão para criar uma associação entre um usuário ou grupo de diretório e um perfil	Gravar			
AttachCustomerManagedPolicyReferenceToPermissionSet	Concede permissão para anexar uma referência de política gerenciada pelo cliente a um conjunto de permissões	Gerenciamento de permissões	Instance* PermissionSet*		
AttachManagedPolic	Concede permissão para anexar uma política AWS	Gerenciamento de	Instance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
yToPermissionSet	gerenciada a um conjunto de permissões	permissões	PermissionSet*		
CreateAccountAssignment	Concede permissão para atribuir acesso a um Diretor para um determinado Conta da AWS usando um conjunto de permissões especificado	Gravar	Account*		
			Instance*		
			PermissionSet*		
CreateApplication	Concede permissão para criar um aplicativo	Gravar	ApplicationProvider*		
			Instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateApplicationAssignment	Concede permissão para criar uma atribuição de aplicação	Gravar	Application*		
				sso:ApplicationAccount	
CreateApplicationInstance	Concede permissão para adicionar uma instância do aplicativo ao AWS IAM Identity Center	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateApplicationInstanceCertificate	Concede permissão para adicionar um novo certificado para uma instância da aplicação	Gravar			
CreateInstance	Concede permissão para criar uma instância de centro de identidade	Gravar	Instance*		iam:CreateServiceLinkedRole organizations:DescribeOrganization
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateInstanceAccessControlAttributeConfiguration	Concede permissão para habilitar a instância para ABAC e especificar os atributos	Gravar	Instance*		iam:AttachRolePolicy iam:CreateRole iam:DeleteRole iam:DeleteRolePolicy iam:DetachRolePolicy iam:GetRole iam:ListAttachedRolePolicies iam:ListRolePolicies iam:PutRolePolicy

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					iam:UpdateAssumeRolePolicy
CreateManagedApplicationInstance	Concede permissão para adicionar uma instância de aplicativo gerenciada ao AWS IAM Identity Center	Gravar			
CreatePermissionSet	Concede permissão para criar um conjunto de permissões	Write	Instance*		
			PermissionSet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfile	Concede permissão para criar um perfil para uma instância da aplicação	Write			
CreateTrust	Concede permissão para criar uma confiança de federação em uma conta de destino	Gravar			
CreateTrustedTokenIssuer	Concede permissão para criar um emissor de token confiável para uma instância	Gravar	Instance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccountAssignment	Concede permissão para excluir o acesso de um diretor de um determinado Conta da AWS usando um conjunto de permissões especificado	Gravar	Account*		
			Instance*		
			PermissionSet*		
DeleteApplication	Concede permissão para excluir um aplicativo	Gravar	Application*		
				sso:ApplicationAccount	
DeleteApplicationAccessScope	Concede permissão para excluir um escopo de acesso para uma aplicação	Gravar	Application*		
				sso:ApplicationAccount	
DeleteApplicationAssignment	Concede permissão para excluir uma atribuição de aplicação	Gravar	Application*		
				sso:ApplicationAccount	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteApplicationAuthenticationMethod	Concede permissão para excluir um método de autenticação para uma aplicação	Gravar	Application*		
				sso:ApplicationAccount	
DeleteApplicationGrant	Concede permissão para excluir uma concessão de uma aplicação	Gravar	Application*		
				sso:ApplicationAccount	
DeleteApplicationInstance	Concede permissão para excluir a instância da aplicação	Write			
DeleteApplicationInstanceCertificate	Concede permissão para excluir um certificado expirado ou inativo da instância da aplicação	Gravar			
DeleteInlinePolicyFromPermissionSet	Concede permissão para excluir a política em linha de um conjunto de permissões especificado	Gravar	Instance*		
			PermissionSet*		
DeleteInstance	Concede permissão para excluir uma instância de centro de identidade	Gravar	Instance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteInstanceAccessControlAttributeConfiguration	Concede permissão para desabilitar o ABAC e remover a lista de atributos da instância	Write	Instance*		
DeleteManagedApplicationInstance	Concede permissão para excluir a instância da aplicação gerenciada	Write			
DeletePermissionSet	Concede permissão para excluir um conjunto de permissões	Gravar	Instance* PermissionSet*		
DeletePermissionsBoundaryFromPermissionSet	Concede permissão para remover limites de permissões de um conjunto de permissões	Gerenciamento de permissões	Instance* PermissionSet*		
DeleteProfile	Concede permissão para excluir o perfil de uma instância da aplicação	Gravar			
DeleteTrustedTokenIssuer	Concede permissão para excluir um emissor de token confiável para uma instância	Gravar	TrustedTokenIssuer*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeAccountAssignmentCreationStatus	Concede permissão para descrever o status da solicitação de criação de atribuição	Leitura	Instance*		
DescribeAccountAssignmentDeletionStatus	Concede permissão para descrever o status de uma solicitação de exclusão da atribuição	Leitura	Instance*		
DescribeApplication	Concede permissão para obter informações sobre uma aplicação	Leitura	Application*		
				sso:ApplicationAccount	
DescribeApplicationAssignment	Concede permissão para recuperar uma atribuição de aplicação	Leitura	Application*		
				sso:ApplicationAccount	
DescribeApplicationProvider	Concede permissão para descrever um provedor de aplicação	Leitura	ApplicationProvider*		
DescribeInstance	Concede permissão para obter informações sobre uma instância de centro de identidade	Leitura	Instance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeInstanceAccessControlAttributeConfiguration	Concede permissão para obter a lista de atributos usados pela instância para ABAC	Read	Instance*		
DescribePermissionSet	Concede permissão para descrever um conjunto de permissões	Leitura	Instance*		
			PermissionSet*		
DescribePermissionSetProvisioningStatus	Concede permissão para descrever o status da solicitação de provisionamento do conjunto de permissões determinado	Leitura	Instance*		
DescribeRegisteredRegions	Concede permissão para obter as regiões em que sua organização habilitou o AWS IAM Identity Center	Leitura			
DescribeTrustedTokenIssuer	Concede permissão para descrever um emissor de token confiável para uma instância	Leitura	TrustedTokenIssuer*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DetachCustomerManagedPolicyReferenceFromPermissionSet	Concede permissão para desvincular uma referência de política gerenciada pelo cliente de um conjunto de permissões	Gerenciamento de permissões	Instance* PermissionSet*		
DetachManagedPolicyFromPermissionSet	Concede permissão para separar a política AWS gerenciada anexada do conjunto de permissões especificado	Gerenciamento de permissões	Instance* PermissionSet*		
DisassociateDirectory	Concede permissão para desassociar um diretório a ser usado pelo AWS IAM Identity Center	Gravar			ds:UnauthorizeApplication
DisassociateProfile	Concede permissão para desassociar um usuário ou grupo de diretório de um perfil	Gravar			
GetApplicationAccessScope	Concede permissão para obter um escopo de acesso para uma aplicação	Leitura	Application* 	 sso:ApplicationAccount	
GetApplicationAssignmentConfiguration	Concede permissão para ler configurações de atribuição para uma aplicação	Leitura	Application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				sso:ApplicationAccount	
GetApplicationAuthenticationMethod	Concede permissão para obter um método de autenticação para uma aplicação	Leitura	Application*		
				sso:ApplicationAccount	
GetApplicationGrant	Concede permissão para obter detalhes sobre uma concessão pertencente a uma aplicação	Leitura	Application*		
				sso:ApplicationAccount	
GetApplicationInstance	Concede permissão para recuperar os detalhes de uma instância da aplicação	Leitura			
GetApplicationSessionConfiguration	Concede permissão para obter a configuração da sessão para um aplicativo	Leitura	Application*		
				sso:ApplicationAccount	
GetApplicationTemplate	Concede permissão para recuperar os detalhes do modelo da aplicação	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetInlinePolicyForPermissionSet	Concede permissão para obter a política em linha atribuída ao conjunto de permissões	Leitura	Instance* PermissionSet*		
GetManagedApplicationInstance	Concede permissão para recuperar os detalhes de uma instância da aplicação	Read			
GetMfaDeviceManagementForDirectory	Concede permissão para recuperar as configurações de gerenciamento de dispositivos MFA para o diretório	Read			
GetPermissionSet	Concede permissão para recuperar detalhes de um conjunto de permissões	Leitura			
GetPermissionsBoundaryForPermissionSet	Concede permissão para obter limites de permissões para um conjunto de permissões	Leitura	Instance* PermissionSet*		
GetProfile	Concede permissão para recuperar um perfil para uma instância da aplicação	Leitura			
GetSSOStatus	Concede permissão para verificar se o AWS IAM Identity Center está ativado	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSharedSsoConfiguration	Concede permissão para recuperar a configuração compartilhada para a instância SSO atual	Read			
GetSsoConfiguration	Concede permissão para recuperar a configuração para a instância atual do SSO	Read			
GetTrust	Concede permissão para recuperar a confiança de federação em uma conta de destino	Read			
ImportApplicationInstanceServiceProviderMetadata	Concede permissão para atualizar a instância da aplicação fazendo upload de um arquivo de metadados SAML da aplicação fornecido pelo provedor de serviços	Gravar			
ListAccountAssignmentCreationStatus	Concede permissão para listar o status das solicitações de criação de Conta da AWS atribuição para uma instância de SSO especificada	Lista	Instance*		
ListAccountAssignmentDeletionStatus	Concede permissão para listar o status das solicitações de exclusão de Conta da AWS atribuição para uma instância de SSO especificada	Lista	Instance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAccountAssignments	Concede permissão para listar o destinatário do especificado Conta da AWS com o conjunto de permissões especificado	Lista	Account*		
			Instance*		
			PermissionSet*		
ListAccountAssignmentsForPrincipal	Concede permissão para listar contas atribuídas a usuário ou grupo	Lista	Instance*		
ListAccountsForProvisionedPermissionSet	Concede permissão para listar todas as AWS contas nas quais o conjunto de permissões especificado é provisionado	Lista	Instance*		
			PermissionSet*		
ListApplicationAccessScopes	Concede permissão para listar escopos de acesso para uma aplicação	Lista	Application*		
				sso:ApplicationAccount	
ListApplicationAssignments	Concede permissão para listar atribuições de aplicação	Lista	Application*		
				sso:ApplicationAccount	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListApplicationAssignmentsForPrincipal	Concede permissão para listar aplicações atribuídas a usuário ou grupo	Lista	Instance*		
				sso:ApplicationAccount	
ListApplicationAuthenticationMethods	Concede permissão para listar métodos de autenticação para uma aplicação	Lista	Application*		
				sso:ApplicationAccount	
ListApplicationGrants	Concede permissão para listar concessões para uma aplicação	Lista	Application*		
				sso:ApplicationAccount	
ListApplicationInstanceCertificates	Concede permissão para recuperar todos os certificados de uma determinada instância da aplicação	Read			
ListApplicationInstances	Concede permissão para recuperar todas as instâncias da aplicação	Lista			sso:GetApplicationInstance
ListApplicationProviders	Concede permissão para listar provedores de aplicação	Lista	ApplicationProvider*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListApplicationTemplates	Concede permissão para recuperar todos os modelos da aplicação com suporte	Lista			sso:GetApplicationTemplate
ListApplications	Concede permissão para recuperar todas as aplicações associadas à instância do IAM Identity Center	Lista			
ListCustomerManagedPolicyReferencesInPermissionSet	Concede permissão para listar as políticas gerenciadas pelo cliente anexadas a um conjunto de permissões	Lista	Instance* PermissionSet*		
ListDirectoryAssociations	Concede permissão para recuperar detalhes sobre o diretório conectado ao AWS IAM Identity Center	Leitura			
ListInstances	Concede permissão para listar as instâncias do SSO às quais o chamador tem acesso	Lista			
ListManagedPoliciesInPermissionSet	Concede permissão para listar as políticas AWS gerenciadas que estão anexadas a um conjunto de permissões especificado	Lista	Instance* PermissionSet*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListPermissionSetProvisioningStatus	Concede permissão para listar o status das solicitações das solicitações de provisionamento do conjunto de permissões de uma instância de SSO especificada	Lista	Instance*		
ListPermissionSets	Concede permissão para recuperar todos os conjuntos de permissões	Lista	Instance*		
ListPermissionSetsProvisionedToAccount	Concede permissão para listar todos os conjuntos de permissões que são provisionados para um determinado Conta da AWS	Lista	Account*		
			Instance*		
ListProfileAssociations	Concede permissão para recuperar o usuário ou grupo de diretório associado ao perfil	Read			
ListProfiles	Concede permissão para recuperar todos os perfis de uma instância da aplicação	Lista			sso:GetProfile
ListTagsForResource	Concede permissão para listar as etiquetas anexadas ao usuário do recurso especificado	Leitura	Application		
			Instance		
			PermissionSet		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			TrustedTokenIssuer		
ListTrustedTokenIssuers	Concede permissão para listar emissores de token confiáveis para uma instância	Lista	Instance*		
ProvisionPermissionSet	Concede permissão para provisionar um conjunto de permissões específico para o destino especificado	Gravar	Account*		
			Instance*		
			PermissionSet*		
PutApplicationAccessScope	Concede permissão a create/update um escopo de acesso a um aplicativo	Gravar	Application*		
				sso:ApplicationAccount	
PutApplicationAssignmentConfiguration	Concede permissão para adicionar configurações de atribuição a uma aplicação	Gravar	Application*		
				sso:ApplicationAccount	
PutApplicationAuthenticationMethod	Concede permissão para create/update um método de autenticação para um aplicativo	Gravar	Application*		
				sso:ApplicationAccount	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutApplicationGrant	Concede permissão a create/update uma concessão a um aplicativo	Gravar	Application*		
				sso:ApplicationAccount	
PutApplicationSessionConfiguration	Concede permissão para colocar a configuração da sessão para um aplicativo	Gravar	Application*		
				sso:ApplicationAccount	
PutInlinePolicyToPermissionSet	Concede permissão para anexar uma política em linha do IAM a um conjunto de permissões	Gravar	Instance*		
			PermissionSet*		
PutMfaDeviceManagementForDirectory	Concede permissão para colocar as configurações de gerenciamento de dispositivos MFA no diretório	Gravar			
PutPermissionsBoundaryToPermissionSet	Concede permissão para adicionar limites de permissões a um conjunto de permissões	Gerenciamento de permissões	Instance*		
			PermissionSet*		
PutPermissionsPolicy	Concede permissão para adicionar uma política a um conjunto de permissões	Permissions management			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SearchGroups	Concede permissão para pesquisar grupos no diretório associado	Read			ds:DescribeDirectories
SearchUsers	Concede permissão para pesquisar usuários no diretório associado	Leitura			ds:DescribeDirectories
StartSSO	Concede permissão para inicializar o AWS IAM Identity Center	Gravar			organizations:DescribeOrganization organizations:EnableAWSServiceAccess
TagResource	Concede permissão para associar um conjunto de etiquetas a um recurso especificado	Tags	Application		
			Instance		
			PermissionSet		
			TrustedTokenIssuer		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desassociar um conjunto de etiquetas de um recurso especificado	Tags	Application		
			Instance		
			PermissionSet		
			TrustedTokenIssuer		
				aws:TagKeys	
UpdateApplication	Concede permissão para atualizar uma aplicação	Gravar	Application*		
				sso:ApplicationAccount	
UpdateApplicationInstanceActiveCertificate	Concede permissão para definir um certificado como ativo para esta instância da aplicação	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateApplicationInstanceDisplayData	Concede permissão para atualizar os dados de exibição de uma instância da aplicação	Write			
UpdateApplicationInstanceResponseConfiguration	Concede permissão para atualizar a configuração da resposta de federação para a instância da aplicação	Write			
UpdateApplicationInstanceResponseSchemaConfiguration	Concede permissão para atualizar o esquema da resposta da federação para a instância da aplicação	Write			
UpdateApplicationInstanceSecurityConfiguration	Concede permissão para atualizar os detalhes de segurança para a instância da aplicação	Write			
UpdateApplicationInstanceServiceProviderConfiguration	Concede permissão para atualizar a configuração relacionada ao provedor do serviço da instância da aplicação	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateApplicationInstanceStatus	Concede permissão para atualizar o status de uma instância da aplicação	Gravar			
UpdateInstance	Concede permissão para atualizar uma instância de centro de identidade	Gravar	Instance*		
UpdateInstanceAccessControlAttributeConfiguration	Concede permissão para atualizar os atributos a serem usados com a instância para ABAC	Write	Instance*		
UpdateManagedApplicationInstanceStatus	Concede permissão para atualizar o status de uma instância da aplicação gerenciada	Gravar			
UpdatePermissionSet	Concede permissão para atualizar o conjunto de permissões	Gerenciamento de permissões	Instance* PermissionSet*		
UpdateProfile	Concede permissão para atualizar o perfil de uma instância da aplicação	Write			
UpdateSSOConfiguration	Concede permissão para atualizar a configuração da instância do SSO atual	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateTrust	Concede permissão para atualizar a confiança de federação em uma conta de destino	Gravar			
UpdateTrustedTokenIssuer	Concede permissão para atualizar um emissor de token confiável para uma instância	Gravar	TrustedTokenIssuer *		

Tipos de recursos definidos pelo AWS IAM Identity Center

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Tipos de recursos	ARN	Chaves de condição
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}`	

Chaves de condição para o AWS IAM Identity Center

AWS O IAM Identity Center define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Chaves de condição	Descrição	Tipo
sso:ApplicationAccount	Filtra o acesso pela conta que cria o aplicativo. Essa chave de condição não é compatível com aplicativos SAML gerenciados pelo cliente	String

Ações, recursos e chaves de condição para o diretório AWS do IAM Identity Center

AWS O diretório do IAM Identity Center (prefixo do serviço:`sso-directory`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo diretório AWS do IAM Identity Center
- Tipos de recursos definidos pelo diretório AWS do IAM Identity Center
- Chaves de condição para o diretório AWS do IAM Identity Center

Ações definidas pelo diretório AWS do IAM Identity Center

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddMemberToGroup	Concede permissão para adicionar um membro a um grupo no diretório que o AWS IAM Identity Center fornece por padrão.	Gravar			
CompleteVirtualMfaDeviceRegistration	Concede permissão para concluir o processo de criação de um dispositivo MFA virtual	Gravar			
CompleteWebAuthnDeviceRegistration	Concede permissão para concluir o processo de registro de um WebAuthn dispositivo	Gravar			
CreateAlias	Concede permissão para criar um alias para o diretório que o AWS IAM Identity Center fornece por padrão	Gravar			
CreateBearerToken	Concede permissão para criar um token de portador para determinado locatário de provisionamento	Write			
CreateExternalIdPConfigurationForDirectory	Concede permissão para criar uma configuração do provedor de identidade externo para o diretório	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateGroup	Concede permissão para criar um grupo no diretório que o AWS IAM Identity Center fornece por padrão	Gravar			
CreateProvisioningTenant	Concede permissão para criar um locatário de provisionamento para determinado diretório	Gravar			
CreateUser	Concede permissão para criar um usuário no diretório que o AWS IAM Identity Center fornece por padrão	Gravar			
DeleteBearerToken	Concede permissão para excluir um token de portador	Write			
DeleteExternalIdPCertificate	Concede permissão para excluir o certificado de IdP externo fornecido	Write			
DeleteExternalIdPConfigurationForDirectory	Concede permissão para excluir uma configuração do provedor de identidade externo associada ao diretório	Gravar			
DeleteGroup	Concede permissão para excluir um grupo do diretório que o AWS IAM Identity Center fornece por padrão	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteMfaDeviceForUser	Concede permissão para excluir um dispositivo MFA por nome de dispositivo para determinado usuário	Write			
DeleteProvisioningTenant	Concede permissão para excluir o locatário de provisionamento	Gravar			
DeleteUser	Concede permissão para excluir um usuário do diretório que o AWS IAM Identity Center fornece por padrão	Gravar			
DescribeDirectory	Concede permissão para recuperar informações sobre o diretório que o AWS IAM Identity Center fornece por padrão	Leitura			
DescribeGroup	Concede permissão para consultar os dados do grupo, não incluindo membros do usuário e do grupo	Leitura			
DescribeGroups	Concede permissão para recuperar informações sobre grupos do diretório que o AWS IAM Identity Center fornece por padrão	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeProvisioningTenant	Concede permissão para descrever o locatário de provisionamento	Leitura			
DescribeUser	Concede permissão para recuperar informações sobre um usuário do diretório que o AWS IAM Identity Center fornece por padrão	Leitura			
DescribeUserByUniqueAttribute	Concede permissão para descrever o usuário com um atributo exclusivo válido representado para o usuário	Leitura			
DescribeUsers	Concede permissão para recuperar informações sobre o usuário do diretório que o AWS IAM Identity Center fornece por padrão	Leitura			
DisableExternalIdPConfigurationForDirectory	Concede permissão para desabilitar a autenticação de usuários finais com um provedor de identidade externo	Gravar			
DisableUser	Concede permissão para desativar um usuário no diretório que o AWS IAM Identity Center fornece por padrão	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
EnableExternalIdPConfigurationForDirectory	Concede permissão para habilitar a autenticação de usuários finais com um provedor de identidade externo	Gravar			
EnableUser	Concede permissão para ativar o usuário no diretório que o AWS IAM Identity Center fornece por padrão	Gravar			
GetAWSSPConfigurationForDirectory	Concede permissão para recuperar as configurações do provedor de serviços do AWS IAM Identity Center para o diretório	Leitura			
GetGroupId	Concede permissão para recuperar informações de ID sobre o grupo do diretório que o AWS IAM Identity Center fornece por padrão	Leitura			
GetUserId	Concede permissão para recuperar informações de ID sobre o usuário do diretório que o AWS IAM Identity Center fornece por padrão	Leitura			
GetUserPoolInfo	(Obsoleto) Concede permissão para obter informações UserPool	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ImportExternalIdPCertificate	Concede permissão para importar o certificado de IdP usado para verificar respostas do IdP externo	Gravar			
IsMemberInGroup	Concede permissão para verificar se um membro faz parte do grupo no diretório que o AWS IAM Identity Center fornece por padrão	Leitura			
IsMemberInGroups	Concede permissão para verificar se um membro faz parte de vários grupos no diretório que o AWS IAM Identity Center fornece por padrão	Leitura			
ListBearerTokens	Concede permissão para listar tokens de portador para determinado locatário de provisionamento	Read			
ListExternalIdPCertificates	Concede permissão para listar certificados do IdP externo de determinados diretório e IdP	Read			
ListExternalIdPConfigurationsForDirectory	Concede permissão para listar todas as configurações do provedor de identidade externo criadas para o diretório	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListGroups	Concede permissão para listar grupos do diretório que o AWS IAM Identity Center fornece por padrão	Leitura			
ListGroupsForMember	Concede permissão para listar os grupos do membro de destino	Leitura			
ListGroupsForUser	Concede permissão para listar grupos para um usuário do diretório que o AWS IAM Identity Center fornece por padrão	Leitura			
ListMembersInGroup	Concede permissão para recuperar todos os membros que fazem parte de um grupo no diretório que o AWS IAM Identity Center fornece por padrão	Leitura			
ListMfaDevicesForUser	Concede permissão para listar todos os dispositivos MFA ativos e seus metadados para um usuário	Read			
ListProvisioningTenants	Concede permissão para listar locatários de provisionamento para determinado diretório	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListUsers	Concede permissão para listar usuários do diretório que o AWS IAM Identity Center fornece por padrão	Leitura			
RemoveMemberFromGroup	Concede permissão para remover um membro que faz parte de um grupo no diretório que o AWS IAM Identity Center fornece por padrão	Gravar			
SearchGroups	Concede permissão para pesquisar grupos no diretório associado	Read			
SearchUsers	Concede permissão para pesquisar usuários no diretório associado	Read			
StartVirtualMfaDeviceRegistration	Concede permissão para iniciar o processo de criação do dispositivo MFA virtual	Gravar			
StartWebAuthnDeviceRegistration	Concede permissão para iniciar o processo de registro de um WebAuthn dispositivo	Gravar			
UpdateExternalIdPConfigurationForDirectory	Concede permissão para atualizar uma configuração do provedor de identidade externo associada ao diretório	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateGroup	Concede permissão para atualizar informações sobre um grupo no diretório que o AWS IAM Identity Center fornece por padrão	Gravar			
UpdateGroupDisplayName	Concede permissão para atualizar a resposta do nome de exibição do grupo	Write			
UpdateMfaDeviceForUser	Concede permissão para atualizar informações do dispositivo MFA	Gravar			
UpdatePassword	Concede permissão para atualizar uma senha enviando um link de redefinição de senha por e-mail ou gerando uma senha de uso único para um usuário no diretório que o AWS IAM Identity Center fornece por padrão	Gravar			
UpdateUser	Concede permissão para atualizar as informações do usuário no diretório que o AWS IAM Identity Center fornece por padrão	Gravar			
UpdateUserName	Concede permissão para atualizar a resposta do nome do usuário	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
VerifyEmail	Concede permissão para verificar um endereço de e-mail de um usuário	Gravar			

Tipos de recursos definidos pelo diretório AWS do IAM Identity Center

AWS O diretório do IAM Identity Center não suporta a especificação de um ARN de recurso no elemento de uma `Resource` declaração de política do IAM. Para permitir o acesso ao diretório AWS do IAM Identity Center, especifique `"Resource": "*"` em sua política.

Chaves de condição para o diretório AWS do IAM Identity Center

O diretório do IAM Identity Center não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o serviço OIDC do Centro de Identidade do AWS IAM

AWS O serviço OIDC do IAM Identity Center (prefixo do serviço:`sso-oauth`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo serviço OIDC do Centro de Identidade do AWS IAM
- Tipos de recursos definidos pelo serviço OIDC do Centro de Identidade do AWS IAM
- Chaves de condição para o serviço OIDC do Centro de Identidade do AWS IAM

Ações definidas pelo serviço OIDC do Centro de Identidade do AWS IAM

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de

recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateTokenWithIAM	Concede permissão para criar OAuth/OIDC tokens para acessar os aplicativos integrados do IAM Identity Center	Gravar	Application*		

Tipos de recursos definidos pelo serviço OIDC do Centro de Identidade do AWS IAM

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
Application	`arn:${Partition}:sso::${AccountId}:application/${InstanceId}/${ApplicationId}`	

Chaves de condição para o serviço OIDC do Centro de Identidade do AWS IAM

O serviço OIDC não possui chaves de contexto específicas ao serviço que possam ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o AWS Identity and Access Management (IAM)

AWS O Identity and Access Management (IAM) (prefixo do serviço`iam`:) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Identity and Access Management (IAM)
- Tipos de recursos definidos pelo AWS Identity and Access Management (IAM)
- Chaves de condição para o AWS Identity and Access Management (IAM)

Ações definidas pelo AWS Identity and Access Management (IAM)

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddClientIDToOpenIDConnectProvider	Concede permissão para adicionar um novo ID de cliente (público) à lista de registrados IDs para o recurso	Gravar	oidc-provider*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	de provedor do IAM OpenID Connect (OIDC) especificado				
AddRoleToInstanceProfile	Concede permissão para adicionar uma função do IAM ao perfil de instância especificado	Write	instance-profile*		iam:PassRole
AddUserToGroup	Concede permissão para adicionar um usuário do IAM ao grupo do IAM especificado	Write	group*		
AttachGroupPolicy	Concede permissão para anexar uma política gerenciada a um grupo do IAM especificado	Permissions management	group*		
				iam:PolicyARN	
AttachRolePolicy	Concede permissão para anexar uma política gerenciada à função do IAM especificada	Permissions management	role*		
				iam:PolicyARN iam:PermissionsBoundary	
AttachUserPolicy	Concede permissão para anexar uma política gerenciada ao usuário do IAM especificado	Gerenciamento de permissões	user*		
				iam:PolicyARN iam:PermissionsBoundary	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ChangePassword	Concede permissão para um usuário do IAM alterar a própria senha	Gravar	user*		
CreateAccessKey	Concede permissão para criar uma chave de acesso e uma chave de acesso secreta para o usuário do IAM especificado	Gravar	user*		
CreateAccountAlias	Concede permissão para criar um alias para seu Conta da AWS	Gravar			
CreateGroup	Concede permissão para criar um grupo	Write	group*		
CreateInstanceProfile	Concede permissão para criar um perfil de instância	Write	instance-profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateLoginProfile	Concede permissão para criar uma senha para o usuário do IAM especificado	Write	user*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateOpenIDConnectProvider	Concede permissão para criar um recurso do IAM que descreve um provedor de identidade (IdP) compatível com OpenID Connect (OIDC)	Write	oidc-provider*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePolicy	Concede permissão para criar uma política gerenciada	Permissions management	policy*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePolicyVersion	Concede permissão para criar uma versão da política gerenciada especificada	Permissions management	policy*		
CreateRole	Concede permissão para criar uma função	Write	role*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				iam:PermissionsBoundary aws:TagKeys aws:RequestTag/${TagKey}	
CreateSAMLProvider	Concede permissão para criar um recurso do IAM que descreve um provedor de identidade (IdP) compatível com SAML 2.0	Gravar	saml-provider*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateServiceLinkedRole	Concede permissão para criar uma função do IAM que permite que um AWS serviço execute ações em seu nome	Gravar	role*		
				iam:AWSServiceName	
CreateServiceSpecificCredential	Concede permissão para criar uma credencial específica do serviço para um usuário do IAM	Write	user*		
CreateUser	Concede permissão para criar um usuário do IAM	Write	user*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				iam:PermissionsBoundary aws:TagKeys aws:RequestTag/${TagKey}	
CreateVirtualMFADevice	Concede permissão para criar um dispositivo MFA virtual	Write	mfa*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeactivateMFADevice	Concede permissão para desativar o dispositivo MFA especificado e remover sua associação com o usuário do IAM para o qual ele foi originalmente habilitado	Write	user*		
DeleteAccessKey	Concede permissão para excluir o par de chaves de acesso associado ao usuário do IAM especificado	Gravar	user*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteAccountAlias	Concede permissão para excluir o Conta da AWS alias especificado	Gravar			
DeleteAccountPasswordPolicy	Concede permissão para excluir a política de senha do Conta da AWS	Gerenciamento de permissões			
DeleteCloudFrontPublicKey	Concede permissão para excluir uma chave CloudFront pública existente	Gravar			
DeleteGroup	Concede permissão para excluir o grupo especificado do IAM	Write	group*		
DeleteGroupPolicy	Concede permissão para excluir a política em linha especificada do grupo	Permissions management	group*		
DeleteInstanceProfile	Concede permissão para excluir o perfil de instância especificado	Write	instance-profile*		
DeleteLoginProfile	Concede permissão para excluir a senha do usuário do IAM especificado	Write	user*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteOpenIDConnectProvider	Concede permissão para excluir um objeto de recurso do provedor de identidade OpenID Connect (IdP) no IAM	Write	oidc-provider*		
DeletePolicy	Concede permissão para excluir a política gerenciada especificada e removê-la de todas as entidades do IAM (usuários, grupos ou funções) às quais ela está anexada	Permissions management	policy*		
DeletePolicyVersion	Concede permissão para excluir uma versão da política gerenciada especificada	Permissions management	policy*		
DeleteRole	Concede permissão para excluir a função especificada	Write	role*		
DeleteRolePermissionsBoundary	Concede permissão para remover o limite de permissões de uma função	Permissions management	role*		
				iam:PermissionsBoundary	
DeleteRolePolicy	Concede permissão para excluir a política em linha especificada da função especificada	Permissions management	role*		
				iam:PermissionsBoundary	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteSAMLProvider	Concede permissão para excluir um recurso de provedor SAML no IAM	Write	saml-provider*		
DeleteSSHPublicKey	Concede permissão para excluir a chave pública SSH especificada	Write	user*		
DeleteServerCertificate	Concede permissão para excluir o certificado de servidor especificado	Gravar	server-certificate*		
DeleteServiceLinkedRole	Concede permissão para excluir uma função do IAM vinculada a um AWS serviço específico, se o serviço não a estiver mais usando	Gravar	role*		
DeleteServiceSpecificCredential	Concede permissão para excluir a credencial específica do serviço especificada para um usuário do IAM	Write	user*		
DeleteSigningCertificate	Concede permissão para excluir um certificado de assinatura associado ao usuário do IAM especificado	Write	user*		
DeleteUser	Concede permissão para excluir o usuário do IAM especificado	Write	user*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteUserPermissionsBoundary	Concede permissão para remover o limite de permissões do usuário do IAM especificado	Permissions management	user*		
				iam:PermissionsBoundary	
DeleteUserPolicy	Concede permissão para excluir a política em linha especificada de um usuário do IAM	Permissions management	user*		
				iam:PermissionsBoundary	
DeleteVirtualMFADevice	Concede permissão para excluir um dispositivo MFA virtual	Write	mfa		
			sms-mfa		
DetachGroupPolicy	Concede permissão para desanexar uma política gerenciada do grupo do IAM especificado	Permissions management	group*		
				iam:PolicyARN	
DetachRolePolicy	Concede permissão para desanexar uma política gerenciada da função especificada	Permissions management	role*		
				iam:PolicyARN iam:PermissionsBoundary	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DetachUserPolicy	Concede permissão para desanexar uma política gerenciada do usuário do IAM especificado	Gerenciamento de permissões	user*		
				iam:PolicyARN iam:PermissionsBoundary	
DisableOrganizationsRootCredentialsManagement	Concede permissão para desativar o gerenciamento das credenciais do usuário raiz da conta do membro para uma organização gerenciada sob a conta atual	Gravar			
DisableOrganizationsRootSessions	Concede permissão para desativar ações raiz privilegiadas em contas de membros de uma organização gerenciada sob a conta atual	Gravar			
EnableMFADevice	Concede permissão para habilitar um dispositivo MFA e associá-lo ao usuário do IAM especificado	Gravar	user*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				iam:RegisterSecurityKey iam:FIDO-FIPS-140-2-certification iam:FIDO-FIPS-140-3-certification iam:FIDO-certification	
EnableOrganizationsRootCredentialsManagement	Concede permissão para permitir o gerenciamento das credenciais do usuário raiz da conta do membro para uma organização gerenciada sob a conta atual	Gravar			
EnableOrganizationsRootSessions	Concede permissão para habilitar ações raiz privilegiadas em contas de membros de uma organização gerenciada sob a conta atual	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GenerateCredentialReport	Concede permissão para gerar um relatório de credenciais para o Conta da AWS	Leitura			
GenerateOrganizationsAccessReport	Concede permissão para gerar um relatório de acesso para uma entidade AWS Organizations	Leitura	access-report*		organizations:DescribePolicy organizations:ListChildren organizations:ListParents organizations:ListPoliciesForTarget organizations:ListRoots organizations:ListTargetsForPolicy

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				iam:OrganizationsPolicyId	
GenerateServiceLastAccessedDetails	Concede permissão para gerar um relatório de dados de serviços acessados mais recentemente de um recurso do IAM	Read	group*		
			policy*		
			role*		
			user*		
GetAccessKeyLastUsed	Concede permissão para recuperar informações sobre quando a chave de acesso foi usada pela última vez	Leitura	user*		
GetAccountAuthorizationDetails	Concede permissão para recuperar informações sobre todos os usuários, grupos, funções e políticas do IAM em seu Conta da AWS, incluindo seus relacionamentos entre si	Leitura			
GetAccountEmailAddress	Concede permissão para recuperar o endereço de e-mail associado à conta	Leitura			
GetAccountName	Concede permissão para recuperar o nome de conta associado à conta	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAccountPasswordPolicy	Concede permissão para recuperar a política de senha do Conta da AWS	Leitura			
GetAccountSummary	Concede permissão para recuperar informações sobre o uso da entidade do IAM e as cotas do IAM no Conta da AWS	Lista			
GetCloudFrontPublicKey	Concede permissão para recuperar informações sobre a chave CloudFront pública especificada	Leitura			
GetContextKeysForCustomPolicy	Concede permissão para recuperar uma lista de todas as chaves de contexto referenciadas na política especificada	Read			
GetContextKeysForPrincipalPolicy	Concede permissão para recuperar uma lista de todas as chaves de contexto referenciadas em todas as políticas do IAM anexadas à identidade do IAM (usuário, grupo ou função)	Leitura	group		
			role		
			user		
GetCredentialReport	Concede permissão para recuperar um relatório de credenciais para o Conta da AWS	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetGroup	Concede permissão para recuperar uma lista de usuários do IAM no grupo do IAM especificado	Read	group*		
GetGroupPolicy	Concede permissão para recuperar um documento de política em linha incorporado no grupo do IAM especificado	Read	group*		
GetInstanceProfile	Concede permissão para recuperar informações sobre o perfil da instância especificada, incluindo o caminho, o GUID, o ARN e a função do perfil da instância	Read	instance-profile*		
GetLoginProfile	Concede permissão para recuperar o nome de usuário e a data de criação da senha do usuário do IAM especificado	Lista	user*		
GetMFADevice	Concede permissão para recuperar informações sobre um dispositivo com MFA para o usuário especificado	Leitura	user*		
GetOpenIDConnectProvider	Concede permissão para recuperar informações sobre o recurso de provedor OpenID Connect (OIDC) no IAM	Leitura	oidc-provider*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetOrganizationsAccessReport	Concede permissão para recuperar um relatório de acesso do AWS Organizations	Leitura			
GetPolicy	Concede permissões para recuperar informações sobre a política gerenciada especificada, incluindo a versão padrão da política e o número total de identidades às quais a política está anexada	Read	policy*		
GetPolicyVersion	Concede permissão para recuperar informações sobre uma versão da política gerenciada especificada, incluindo o documento de política	Read	policy*		
GetRole	Concede permissão para recuperar informações sobre a função especificada incluindo o caminho, o GUID, o ARN e a política de confiança da função	Read	role*		
GetRolePolicy	Concede permissão para recuperar um documento de política em linha incorporado à função do IAM especificada	Read	role*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSAMLProvider	Concede permissão para recuperar o metadocumento do provedor SAML que foi obtido por upload quando o objeto do recurso do provedor SAML do IAM foi criado ou atualizado	Read	saml-provider*		
GetSSHPublicKey	Concede permissão para recuperar a chave pública SSH especificada, incluindo metadados sobre a chave	Read	user*		
GetServerCertificate	Concede permissão para recuperar informações sobre o certificado de servidor especificado, armazenado no IAM	Read	server-certificate*		
GetServiceLastAccessedDetails	Concede permissão para recuperar informações sobre o relatório de dados de serviços acessados mais recentemente	Read			
GetServiceLastAccessedDetailsWithEntities	Concede permissão para recuperar informações sobre as entidades do relatório de dados de serviços acessados mais recentemente	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetServiceLinkedRoleDeletionStatus	Concede permissão para recuperar o status de exclusão de uma função vinculada ao serviço do IAM	Read	role*		
GetUser	Concede permissão para recuperar informações sobre o usuário do IAM especificado, incluindo a data de criação do usuário, o caminho, o ID exclusivo e o ARN	Read	user*		
GetUserPolicy	Concede permissão para recuperar um documento de política em linha incorporado no usuário do IAM especificado	Leitura	user*		
ListAccessKeys	Concede permissão para listar informações sobre a chave de acesso IDs que estão associadas ao usuário do IAM especificado	Lista	user*		
ListAccountAliases	Concede permissão para listar o alias da conta que está associado ao Conta da AWS	Lista			
ListAttachedGroupPolicies	Concede permissão para listar todas as políticas gerenciadas anexadas ao grupo do IAM especificado	List	group*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAttachedRolePolicies	Concede permissão para listar todas as políticas gerenciadas anexadas à função do IAM especificada	List	role*		
ListAttachedUserPolicies	Concede permissão para listar todas as políticas gerenciadas anexadas ao usuário do IAM especificado	Lista	user*		
ListCloudFrontPublicKeys	Concede permissão para listar todas as chaves CloudFront públicas atuais da conta	Lista			
ListEntitiesForPolicy	Concede permissão para listar todas as identidades do IAM às quais a política gerenciada especificada está anexada	List	policy*		
ListGroupPolicies	Concede permissão para listar os nomes das políticas em linha incorporadas no grupo do IAM especificado	List	group*		
ListGroups	Concede permissão para listar os grupos do IAM que possuem o prefixo do caminho especificado	List			
ListGroupsForUser	Concede permissão para listar os grupos do IAM aos quais o usuário do IAM especificado pertence	List	user*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListInstanceProfileTags	Concede permissão para listar as etiquetas anexadas ao perfil de instância especificado	List	instance-profile*		
ListInstanceProfiles	Concede permissão para listar os perfis de instância que possuem o prefixo do caminho especificado	List			
ListInstanceProfilesForRole	Concede permissão para listar os perfis de instância que têm a função do IAM especificada	List	role*		
ListMFADeviceTags	Concede permissão para listar as etiquetas anexadas ao dispositivo MFA virtual especificado.	List	mfa*		
ListMFADevices	Concede permissão para listar os dispositivos MFA de um usuário do IAM	List	user		
ListOpenIDConnectProviderTags	Concede permissão para listar as etiquetas anexadas ao provedor OpenID Connect especificado	Lista	oidc-provider*		
ListOpenIDConnectProviders	Concede permissão para listar informações sobre os objetos de recursos do provedor IAM OpenID Connect (OIDC) que estão definidos no Conta da AWS	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListOrganizationsFeatures	Concede permissão para listar os recursos de acesso root centralizado habilitados para sua organização	Lista			
ListPolicies	Concede permissão para listar todas as políticas gerenciadas	List			
ListPoliciesGrantingServiceAccess	Concede permissão para listar informações sobre as políticas que concedem à entidade o acesso a um serviço específico	List	group*		
			role*		
			user*		
ListPolicyTags	Concede permissão para listar as etiquetas anexadas à política gerenciada especificada.	List	policy*		
ListPolicyVersions	Concede permissão para listar informações sobre as versões da política gerenciada especificada, incluindo a versão que está definida atualmente como a versão padrão da política	List	policy*		
ListRolePolicies	Concede permissão para listar os nomes das políticas em linha incorporadas na função do IAM especificada	List	role*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListRoleTags	Concede permissão para listar as etiquetas anexadas à função do IAM especificada	List	role*		
ListRoles	Concede permissão para listar as funções do IAM que têm o prefixo do caminho especificado	List			
ListSAMLProviderTags	Concede permissão para listar as etiquetas anexadas ao usuário do provedor SAML especificado	List	saml-provider*		
ListSAMLProviders	Concede permissão para listar os recursos de provedor SAML no IAM	List			
ListSSHPublicKeys	Concede permissão para listar informações sobre as chaves públicas SSH associadas ao usuário do IAM especificado	Lista	user*		
ListSTSRegionalEndpointsStatus	Concede permissão para listar o status de todos os endpoints regionais ativos do STS	Lista			
ListServerCertificateTags	Concede permissão para listar as etiquetas anexadas ao certificado do servidor especificado	List	server-certificate*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListServerCertificates	Concede permissão para listar os certificados de servidor que têm o prefixo do caminho especificado	List			
ListServiceSpecificCredentials	Concede permissão para listar as credenciais específicas do serviço associadas ao usuário do IAM especificado	List	user*		
ListSigningCertificates	Concede permissão para listar informações sobre os certificados de assinatura associados ao usuário do IAM especificado	List	user*		
ListUserPolicies	Concede permissão para listar os nomes das políticas em linha incorporadas no usuário do IAM especificado	List	user*		
ListUserTags	Concede permissão para listar as etiquetas anexadas ao usuário do IAM especificado	List	user*		
ListUsers	Concede permissão para listar os usuários do IAM que têm o prefixo do caminho especificado	List			
ListVirtualMFADevices	Concede permissão para listar dispositivos MFA virtuais por status de atribuição	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PassRole [somente permissão]	Concede permissão para transmitir uma função para um serviço	Write	role*		
				iam:AssociatedResourceArn iam:PassedToService	
PutGroupPolicy	Concede permissão para criar ou atualizar um documento de política em linha incorporado no grupo do IAM especificado	Permissions management	group*		
PutRolePermissionsBoundary	Concede permissão para definir uma política gerenciada como um limite de permissões para uma função	Permissions management	role*		
				iam:PermissionsBoundary	
PutRolePolicy	Concede permissão para criar ou atualizar um documento de política em linha incorporado na função do IAM especificada	Permissions management	role*		
				iam:PermissionsBoundary	
PutUserPermissionsBoundary	Concede permissão para definir uma política gerenciada como um limite de permissões para um usuário do IAM	Permissions management	user*		
				iam:PermissionsBoundary	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutUserPolicy	Concede permissão para criar ou atualizar um documento de política em linha incorporado no usuário do IAM especificado	Gerenciamento de permissões	user*		
				iam:PermissionsBoundary	
RemoveClientIDFromOpenIDConnectProvider	Concede permissão para remover o ID do cliente (público) da lista de clientes IDs no recurso de provedor do IAM OpenID Connect (OIDC) especificado	Gravar	oidc-provider*		
RemoveRoleFromInstanceProfile	Concede permissão para remover uma função do IAM do perfil de EC2 instância especificado	Gravar	instance-profile*		
RemoveUserFromGroup	Concede permissão para remover um usuário do IAM do grupo especificado	Write	group*		
ResetServiceSpecificCredential	Concede permissão para redefinir a senha de uma credencial existente específica do serviço de um usuário do IAM	Write	user*		
ResyncMFADevice	Concede permissão para sincronizar o dispositivo MFA especificado com a entidade do IAM (usuário ou função)	Write	user*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SetDefaultPolicyVersion	Concede permissão para definir a versão da política especificada como a versão padrão da política	Gerenciamento de permissões	policy*		
SetSTSRegionalEndpointStatus	Concede permissão para ativar ou desativar um endpoint regional do STS	Gravar			
SetSecurityTokenServicePreferences	Concede permissão para definir a versão do token do endpoint global do STS	Write			
SimulateCustomPolicy	Concede permissão para simular se uma política baseada em identidade ou uma política baseada em recurso fornece permissões para operações e recursos de API específicos	Read			
SimulatePrincipalPolicy	Concede permissão para simular se uma política baseada em identidade anexada a uma entidade do IAM (usuário ou função) especificada fornece permissões para recursos e operações de API específicos	Read	group		
			role		
			user		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagInstanceProfile	Concede permissão para adicionar etiquetas a um perfil de instância	Marcação	instance-profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagMFADevice	Concede permissão para adicionar etiquetas a um dispositivo MFA virtual	Marcação	mfa*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagOpenIDConnectProvider	Concede permissão para adicionar etiquetas a um provedor OpenID Connect	Marcação	oidc-provider*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagPolicy	Concede permissão para adicionar etiquetas a uma política gerenciada	Marcação	policy*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
TagRole	Concede permissão para adicionar etiquetas a uma função do IAM	Marcação	role*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagSAMLProvider	Concede permissão para adicionar etiquetas a um provedor SAML	Marcação	saml-provider*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagServerCertificate	Concede permissão para adicionar etiquetas a um certificado do servidor	Marcação	server-certificate*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
TagUser	Concede permissão para adicionar etiquetas a um usuário do IAM	Marcação	user*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagInstanceProfile	Concede permissão para remover as etiquetas especificadas do perfil de instância	Marcação	instance-profile*		
				aws:TagKeys	
UntagMFADevice	Concede permissão para remover as etiquetas especificadas do dispositivo MFA virtual	Marcação	mfa*		
				aws:TagKeys	
UntagOpenIDConnectProvider	Concede permissão para remover as etiquetas especificadas do provedor OpenID Connect	Marcação	oidc-provider*		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagPolicy	Concede permissão para remover as etiquetas especificadas da política gerenciada	Marcação	policy*		
				aws:TagKeys	
UntagRole	Concede permissão para remover as etiquetas especificadas da função	Marcação	role*		
				aws:TagKeys	
UntagSAMLProvider	Concede permissão para remover as etiquetas especificadas do provedor SAML	Marcação	saml-provider*		
				aws:TagKeys	
UntagServerCertificate	Concede permissão para remover as etiquetas especificadas do certificado do servidor	Marcação	server-certificate*		
				aws:TagKeys	
UntagUser	Concede permissão para remover as etiquetas especificadas do usuário	Marcação	user*		
				aws:TagKeys	
UpdateAccessKey	Concede permissão para atualizar o status da chave de acesso especificada como ativa ou inativa	Gravar	user*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateAccountEmailAddress	Concede permissão para atualizar o endereço de e-mail associado à conta	Gravar			
UpdateAccountName	Concede permissão para atualizar o nome de conta associado à conta	Gravar			
UpdateAccountPasswordPolicy	Concede permissão para atualizar as configurações da política de senha do Conta da AWS	Gravar			
UpdateAssumeRolePolicy	Concede permissão para atualizar a política que concede a uma entidade do IAM permissão para assumir uma função	Gerenciamento de permissões	role*		
UpdateCloudFrontPublicKey	Concede permissão para atualizar uma chave CloudFront pública existente	Gravar			
UpdateGroup	Concede permissão para atualizar o nome ou o caminho do grupo do IAM especificado	Write	group*		
UpdateLoginProfile	Concede permissão para alterar a senha do usuário do IAM especificado	Write	user*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateOpenIDConnectProviderThumbprint	Concede permissão para atualizar toda a lista de thumbprints de certificado de servidor associados a um recurso de provedor OpenID Connect (OIDC)	Write	oidc-provider*		
UpdateRole	Concede permissão para atualizar a descrição ou configuração de duração máxima da sessão de uma função	Write	role*		
UpdateRoleDescription	Concede permissão para atualizar somente a descrição de uma função	Write	role*		
UpdateSAMLProvider	Concede permissão para atualizar o documento de metadados de um recurso de provedor SAML existente	Write	saml-provider*		
UpdateSSHPublicKey	Concede permissão para atualizar o status de uma chave pública SSH do usuário do IAM para ativo ou inativo	Write	user*		
UpdateServerCertificate	Concede permissão para atualizar o nome ou o caminho do certificado de servidor especificado, armazenado no IAM	Write	server-certificate*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateServiceSpecificCredential	Concede permissão para atualizar o status de uma credencial específica do serviço como ativo ou inativo para um usuário do IAM	Write	user*		
UpdateSigningCertificate	Concede permissão para atualizar o status do certificado de assinatura do usuário especificado para ativo ou desativado	Write	user*		
UpdateUser	Concede permissão para atualizar o nome ou o caminho do usuário do IAM especificado	Gravar	user*		
UploadCloudFrontPublicKey	Concede permissão para fazer upload de uma chave CloudFront pública	Gravar			
UploadSSHPublicKey	Concede permissão para fazer upload de uma chave pública SSH e associá-la ao usuário do IAM especificado	Gravar	user*		
UploadServerCertificate	Concede permissão para carregar uma entidade certificada de servidor para o Conta da AWS	Gravar	server-certificate*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
UploadSigningCertificate	Concede permissão para fazer upload de um certificado de assinatura X.509 e associá-lo ao usuário do IAM especificado	Gravar	user*		

Tipos de recursos definidos pelo AWS Identity and Access Management (IAM)

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
access-report	`arn:${Partition}:iam::${Account}:access-report/${EntityPath}`	
assumed-role	`arn:${Partition}:iam::${Account}:assumed-role/${RoleName}/${RoleSessionName}`	

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
user	`arn:${Partition}:iam::${Account}:user/${UserNameWithPath}`	aws:ResourceTag/${TagKey} iam:ResourceTag/${TagKey}

Chaves de condição para o AWS Identity and Access Management (IAM)

AWS O Identity and Access Management (IAM) define as seguintes chaves de condição que podem ser usadas no elemento de uma `Condition` política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base nas etiquetas transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra as ações com base nas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra ações com base nas chaves da etiqueta transmitidas na solicitação	ArrayOfString
iam:AWSServiceName	Filtra o acesso pelo AWS serviço ao qual essa função está vinculada	String
iam:AssociatedResourceArn	Filtra o acesso pelo recurso em nome do qual o perfil será usado	ARN

Chaves de condição	Descrição	Type
iam:FIDO-FIPS-140-2-certification	Filtra o acesso pelo nível de certificação de validação FIPS-140-2 do dispositivo com MFA no momento do registro de uma chave de segurança FIDO	String
iam:FIDO-FIPS-140-3-certification	Filtra o acesso pelo nível de certificação de validação FIPS-140-3 do dispositivo MFA no momento do registro de uma chave de segurança FIDO	String
iam:FIDO-certification	Filtra o acesso pelo nível de certificação FIDO do dispositivo com MFA no momento do registro de uma chave de segurança FIDO	String
iam:OrganizationsPolicyId	Filtra o acesso pelo ID de uma política da AWS Organizations	String
iam:PassedToService	Filtra o acesso pelo AWS serviço para o qual essa função é passada	String
iam:PermissionsBoundary	Filtra o acesso se a política especificada está definida como o limite de permissões na entidade do IAM (usuário ou função)	ARN
iam:PolicyARN	Filtra o acesso pelo ARN de uma política do IAM	ARN
iam:RegisterSecurityKey	Filtra o acesso pelo estado atual da ativação do dispositivo com MFA	String
iam:ResourceTag/${TagKey}	Filtra acesso pelas etiquetas anexadas a uma entidade do IAM (usuário ou função)	String

Ações, recursos e chaves de condição para o AWS Identity and Access Management Roles Anywhere

AWS O Identity and Access Management Roles Anywhere (prefixo do serviço:`rolesanywhere`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Identity and Access Management Roles Anywhere
- Tipos de recursos definidos pelo AWS Identity and Access Management Roles Anywhere
- Chaves de condição do AWS Identity and Access Management Roles Anywhere

Ações definidas pelo AWS Identity and Access Management Roles Anywhere

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa

ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateProfile	Concede permissão para criar um perfil	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
CreateTrustAnchor	Concede permissão para criar uma âncora de confiança	Gravar		aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
DeleteAttributeMapping	Concede permissão para excluir uma regra de mapeamento de um perfil	Gravar	profile*		
DeleteCrl	Concede permissão para excluir uma lista de revogação de certificados (crl)	Gravar	crl*		
DeleteProfile	Concede permissão para excluir um perfil	Gravar	profile*		
DeleteTrustAnchor	Concede permissão para excluir uma âncora de confiança	Gravar	trust-anchor*		
DisableCrl	Concede permissão para desabilitar uma lista de revogação de certificados (crl)	Gravar	crl*		
DisableProfile	Concede permissão para desabilitar um perfil	Gravar	profile*		
DisableTrustAnchor	Concede permissão para desabilitar uma âncora de confiança	Gravar	trust-anchor*		
EnableCrl	Concede permissão para habilitar uma lista de revogação de certificados (crl)	Gravar	crl*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
EnableProfile	Concede permissão para habilitar um perfil	Gravar	profile*		iam:PassRole
EnableTrustAnchor	Concede permissão para habilitar uma âncora de confiança	Gravar	trust-anchor*		
GetCrl	Concede permissão para obter uma lista de revogação de certificados (crl)	Leitura	crl*		
GetProfile	Concede permissão para obter um perfil	Leitura	profile*		
GetSubject	Concede permissão para obter um assunto	Leitura	subject*		
GetTrustAnchor	Concede permissão para obter uma âncora de confiança	Leitura	trust-anchor*		
ImportCrl	Concede permissão para importar uma lista de revogação de certificados (crl)	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
ListCrls	Concede permissão para listar listas de revogação de certificados (crls)	Lista			
ListProfiles	Concede permissão para listar perfis	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListSubjects	Concede permissão para listar assuntos	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Lista			
ListTrustAnchors	Concede permissão para listar âncoras de confiança	Lista			
PutAttributeMapping	Concede permissão para colocar uma regra de mapeamento em um perfil	Gravar	profile*		
PutNotificationSettings	Concede permissão para anexar configurações de notificação a uma âncora de confiança	Gravar	trust-anchor*		
ResetNotificationSettings	Concede permissão para redefinir as configurações de notificação personalizada para o estado padrão definido pelo IAM Roles Anywhere	Gravar	trust-anchor*		
TagResource	Concede permissão para marcar um recurso	Marcação	crl		
			profile		
			subject		
			trust-anchor		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso	Tags	crl		
			profile		
			subject		
			trust-anchor		
				aws:TagKeys	
UpdateCrl	Concede permissão para atualizar uma lista de revogação de certificados (crl)	Gravar	crl*		
UpdateProfile	Concede permissão para atualizar um perfil	Gravar	profile*		iam:PassRole
UpdateTrustAnchor	Concede permissão para atualizar uma âncora de confiança	Gravar	trust-anchor*		

Tipos de recursos definidos pelo AWS Identity and Access Management Roles Anywhere

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS Identity and Access Management Roles Anywhere

AWS O Identity and Access Management Roles Anywhere define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Identity Store

AWS O Identity Store (prefixo do serviço:`identitystore`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Identity Store
- Tipos de recursos definidos pelo AWS Identity Store
- Chaves de condição do AWS Identity Store

Ações definidas pelo AWS Identity Store

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateGroup	Concede permissão para criar um grupo no especificado IdentityStore	Gravar	Identitystore*		
CreateGroupMembership	Concede permissão para criar um membro para um grupo na área especificada IdentityStore	Gravar	Group*		
			Identitystore*		
			User*		
CreateUser	Concede permissão para criar um usuário no especificado IdentityStore	Gravar	Identitystore*		
DeleteGroup	Concede permissão para excluir um grupo no especificado IdentityStore	Gravar	Group*		
			Identitystore*		
DeleteGroupMembership	Concede permissão para remover um membro que faz parte de um grupo na área especificada IdentityStore	Gravar	Group*		
			GroupMembership*		
			Identitystore*		
			User*		
DeleteUser	Concede permissão para excluir um usuário no especificado IdentityStore	Gravar	Identitystore*		
			User*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeGroup	Concede permissão para recuperar informações sobre um grupo no especificado IdentityStore	Leitura	Group*		
			Identitystore*		
DescribeGroupMembership	Concede permissão para recuperar informações sobre um membro que faz parte de um grupo no especificado IdentityStore	Leitura	Group*		
			GroupMembership*		
			Identitystore*		
			User*		
DescribeUser	Concede permissão para recuperar informações sobre o usuário no especificado IdentityStore	Leitura	Identitystore*		
			User*		
GetGroupId	Concede permissão para recuperar informações de ID sobre o grupo no especificado IdentityStore	Leitura	Group*		
			Identitystore*		
GetGroupMembershipId	Concede permissão para recuperar informações de ID de um membro que faz parte de um grupo no especificado IdentityStore	Leitura	Group*		
			GroupMembership*		
			Identitystore*		
			User*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetUserId	Concede permissão para recuperar informações de ID sobre o usuário no especificado IdentityStore	Leitura	Identitystore*		
			User*		
IsMemberInGroups	Concede permissão para verificar se um membro faz parte de grupos na área especificada IdentityStore	Leitura	AllGroupMemberships*		
			Group*		
			Identitystore*		
			User*		
ListGroupMemberships	Concede permissão para recuperar todos os membros que fazem parte de um grupo na área especificada IdentityStore	Lista	AllGroupMemberships*		
			Group*		
			Identitystore*		
ListGroupMembershipsForMember	Concede permissão para listar grupos do membro de destino no especificado IdentityStore	Lista	AllGroupMemberships*		
			Identitystore*		
			User*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListGroups	Concede permissão para pesquisar grupos dentro do especificado IdentityStore	Lista	AllGroups*		
			Identitystore*		
ListUsers	Concede permissão para pesquisar usuários no campo especificado IdentityStore	Lista	AllUsers*		
			Identitystore*		
UpdateGroup	Concede permissão para atualizar informações sobre um grupo no especificado IdentityStore	Gravar	Group*		
			Identitystore*		
UpdateUser	Concede permissão para atualizar as informações do usuário no especificado IdentityStore	Gravar	Identitystore*		
			User*		

Tipos de recursos definidos pelo AWS Identity Store

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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/*	

Chaves de condição do AWS Identity Store

AWS O Identity Store define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
identitystore:UserId	Filtra o acesso pelo ID de usuário do IAM Identity Center	String

Ações, recursos e chaves de condição do AWS Identity Store Auth

AWS O Identity Store Auth (prefixo do serviço:`identitystore-auth`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Identity Store Auth
- Tipos de recursos definidos pelo AWS Identity Store Auth
- Chaves de condição para o AWS Identity Store Auth

Ações definidas pelo AWS Identity Store Auth

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o

nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchDeleteSession	Concede permissão para excluir um lote de sessões específicas	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
[somente permissão]					
BatchGetSession [somente permissão]	Concede permissão para retornar atributos de sessão para um lote de sessões específicas	Leitura			
ListSessions [somente permissão]	Concede permissão para recuperar uma lista de sessões ativas para um usuário específico	Lista			

Tipos de recursos definidos pelo AWS Identity Store Auth

AWS O Identity Store Auth não suporta a especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para permitir acesso ao AWS Identity Store Auth, especifique `"Resource": "*"` em sua política.

Chaves de condição para o AWS Identity Store Auth

O Identity Store Auth não tem chaves de contexto específicas do serviço que possam ser usadas no elemento `Condition` de instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o AWS Identity Sync

AWS O Identity Sync (prefixo do serviço:`identity-sync`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.

- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Identity Sync
- Tipos de recursos definidos pelo AWS Identity Sync
- Chaves de condição do AWS Identity Sync

Ações definidas pelo AWS Identity Sync

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AllowVendedLogDeliveryForResource [somente permissão]	Concede permissão para configurar a entrega de logs fornecidos para um perfil de sincronização	Gerenciamento de permissões	SyncProfileResource*		
CreateSyncFilter	Concede permissão para criar um filtro de sincronização no perfil de sincronização	Gravar	SyncProfileResource*		
CreateSyncProfile	Concede permissão para criar um perfil de sincronização para a fonte de identidades	Gravar			ds:AuthorizeApplication
CreateSyncTarget	Concede permissão para criar um destino de sincronização para a fonte de identidades	Gravar	SyncProfileResource*		
DeleteSyncFilter	Concede permissão para excluir um filtro de sincroniz	Gravar	SyncProfileResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	ação do perfil de sincronização				
DeleteSyncProfile	Concede permissão para excluir um perfil de sincronização da origem	Gravar	SyncProfileResource*		ds:UnauthorizeApplication
DeleteSyncTarget	Concede permissão para excluir um destino de sincronização da origem	Gravar	SyncProfileResource*		
			SyncTargetResource*		
GetSyncProfile	Concede permissão para recuperar um perfil de sincronização usando um nome do perfil de sincronização	Leitura	SyncProfileResource*		
GetSyncTarget	Concede permissão para recuperar um destino de sincronização do perfil de sincronização	Leitura	SyncProfileResource*		
			SyncTargetResource*		
ListSyncFilters	Concede permissão para listar os filtros de sincronização do perfil de sincronização	Lista	SyncProfileResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartSync	Concede permissão para iniciar um processo de sincronização ou para retomar um processo de sincronização pausado anteriormente	Gravar	SyncProfileResource*		
StopSync	Concede permissão para interromper qualquer processo de sincronização planejado no cronograma de sincronização desde o início	Gravar	SyncProfileResource*		
UpdateSyncTarget	Concede permissão para atualizar um destino de sincronização do perfil de sincronização	Gravar	SyncProfileResource*		
			SyncTargetResource*		

Tipos de recursos definidos pelo AWS Identity Sync

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
SyncProfileResource	`arn:${Partition}:identity-sync:${Region}:${Account}:profile/${SyncProfileName}`	
SyncTargetResource	`arn:${Partition}:identity-sync:${Region}:${Account}:target/${SyncProfileName}/${SyncTargetName}`	

Chaves de condição do AWS Identity Sync

O Identity Sync não tem chaves de contexto específicas do serviço que possam ser usadas no elemento `Condition` de instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Import Export Disk Service

AWS O Import Export Disk Service (prefixo do serviço:`importexport`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Import Export Disk Service
- Tipos de recursos definidos pelo AWS Import Export Disk Service
- Chaves de condição do AWS Import Export Disk Service

Ações definidas pelo AWS Import Export Disk Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelJob	Esta ação cancela um trabalho especificado. Somente o proprietário do trabalho pode cancelá-lo. A ação falhará se o trabalho já tiver começado ou estiver completo.	Write			
CreateJob	Esta ação inicia o processo de agendar um upload ou download dos seus dados.	Gravar			
GetShippingLabel	Essa ação gera uma etiqueta de frete pré-paga que você usará para enviar seu dispositivo AWS para processamento.	Leitura			
GetStatus	Essa ação retorna informações sobre um trabalho, incluindo onde ele se encontra no pipeline de processamento, o status dos resultados e o valor da assinatura associado ao trabalho.	Read			
ListJobs	Essa ação retorna os trabalhos associados ao solicitante.	List			
UpdateJob	Você pode usar essa ação para alterar os parâmetros	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	especificados no arquivo de manifesto original, fornecendo um novo arquivo de manifesto.				

Tipos de recursos definidos pelo AWS Import Export Disk Service

AWS O Import Export Disk Service não suporta a especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para conceder acesso ao AWS Import Export Disk Service, especifique `"Resource": "*"` na política.

Chaves de condição do AWS Import Export Disk Service

O Import/Export não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do Amazon Inspector

O Amazon Inspector (prefixo do serviço: `inspector`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Inspector
- Tipos de recursos definidos pelo Amazon Inspector
- Chaves de condição do Amazon Inspector

Ações definidas pelo Amazon Inspector

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddAttributesToFindings	Concede permissão para atribuir atributos (pares de chave e valor) às descobertas que são ARNs especificadas pelas descobertas	Gravar			
CreateAssessmentTarget	Concede permissão para criar um novo alvo de avaliação usando o ARN do grupo de recursos gerado pelo CreateResourceGroup	Gravar			
CreateAssessmentTemplate	Concede permissão para criar um modelo de avaliação para o destino de avaliação que é especificada pelo ARN do destino de avaliação	Write			
CreateExclusionsPreview	Concede permissão para iniciar a geração de uma visualização de exclusões para o modelo de avaliação especificado	Gravar			
CreateResourceGroup	Concede permissão para criar um grupo de recursos usando o conjunto especificado de tags (pares de chaves e valores) que são usados para selecionar as EC2 instâncias a serem incluídas em um	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	alvo de avaliação do Amazon Inspector				
DeleteAssessmentRun	Concede permissão para excluir a execução de avaliação especificada pelo ARN da execução de avaliação	Write			
DeleteAssessmentTarget	Concede permissão para excluir o destino de avaliação especificado pelo ARN do destino de avaliação	Write			
DeleteAssessmentTemplate	Concede permissão para excluir o modelo de avaliação que é especificado pelo ARN do modelo de avaliação	Gravar			
DescribeAssessmentRuns	Concede permissão para descrever as execuções de avaliação especificadas pelas execuções ARNs de avaliação	Leitura			
DescribeAssessmentTargets	Concede permissão para descrever as metas de avaliação que são especificadas pelas metas ARNs de avaliação	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeAssessmentTemplates	Concede permissão para descrever os modelos de avaliação que são especificados pelos modelos ARNs de avaliação	Leitura			
DescribeCrossAccountAccessRole	Concede permissão para descrever a função do IAM que permite que o Amazon Inspector acesse seu Conta da AWS	Leitura			
DescribeExclusions	Concede permissão para descrever as exclusões especificadas pelas 'exclusões' ARNs	Leitura			
DescribeFindings	Concede permissão para descrever as descobertas que são especificadas pela ARNs das descobertas	Leitura			
DescribeResourceGroups	Concede permissão para descrever os grupos de recursos que são especificados pelo ARNs dos grupos de recursos	Leitura			
DescribeRulesPackages	Concede permissão para descrever os pacotes de regras especificados pelo ARNs dos pacotes de regras	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAssessmentReport	Concede permissão para gerar um relatório de avaliação que inclua resultados detalhados e abrangentes de uma execução de avaliação especificada	Leitura			
GetExclusionsPreview	Concede permissão para recuperar a visualização prévia das exclusões (uma lista de ExclusionPreview objetos) especificada pelo token de visualização	Leitura			
GetTelemetryMetadata	Concede permissão para obter informações sobre os dados que são coletados para a execução de avaliação especificada	Leitura			
ListAssessmentRunAgents	Concede permissão para listar os agentes das execuções de avaliação que são especificados pelas execuções ARNs de avaliação	Lista			
ListAssessmentRuns	Concede permissão para listar as execuções de avaliação que correspondem aos modelos de avaliação especificados pelos modelos ARNs de avaliação	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAssessmentTargets	Concede permissão para listar os alvos ARNs de avaliação dentro deste Conta da AWS	Lista			
ListAssessmentTemplates	Concede permissão para listar os modelos de avaliação que correspondem às metas de avaliação especificadas pelas metas ARNs de avaliação.	Lista			
ListEventSubscriptions	Concede permissão para listar todas as inscrições de eventos para o modelo de avaliação que é especificado pelo ARN do modelo de avaliação	List			
ListExclusions	Concede permissão para listar exclusões geradas pela execução de avaliação	Lista			
ListFindings	Concede permissão para listar as descobertas geradas pelas execuções de avaliação que são especificadas pelas execuções ARNs de avaliação	Lista			
ListRulesPackages	Concede permissão para listar todos os pacotes de regras disponíveis do Amazon Inspector	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar todas as etiquetas associadas a um modelo de avaliação	Leitura			
PreviewAgents	Concede permissão para visualizar os agentes instalados nas EC2 instâncias que fazem parte da meta de avaliação especificada	Leitura			
RegisterCrossAccountAccessRole	Concede permissão para registrar a função do IAM que o Amazon Inspector usa para listar suas EC2 instâncias no início da execução da avaliação ou quando você chama a ação PreviewAgents	Gravar			
RemoveAttributesFromFindings	Concede permissão para remover atributos inteiros (pares de chave e valor) das descobertas que são especificadas pelas ARNs descobertas em que existe um atributo com a chave especificada	Gravar			
SetTagsForResource	Concede permissão para definir etiquetas (pares de chave e valor) para o modelo de avaliação que é especificado pelo ARN do modelo de avaliação	Marcação			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartAssessmentRun	Concede permissão para iniciar a execução de avaliação especificada pelo ARN do modelo de avaliação	Write			
StopAssessmentRun	Concede permissão para interromper a execução da avaliação especificada pelo ARN da execução de avaliação	Write			
SubscribeToEvent	Concede permissão para ativar o processo de envio de notificações do Amazon Simple Notification Service (SNS) sobre um evento especificado para um tópico do SNS especificado	Write			
UnsubscribeFromEvent	Concede permissão para desativar o processo de envio de notificações do Amazon Simple Notification Service (SNS) sobre um evento especificado para um tópico do SNS especificado	Write			
UpdateAssessmentTarget	Concede permissão para atualizar o destino de avaliação especificado pelo ARN do destino de avaliação	Write			

Tipos de recursos definidos pelo Amazon Inspector

O Amazon Inspector não oferece suporte à especificação do ARN de um recurso no elemento `Resource` de uma instrução de política do IAM. Para conceder acesso ao Amazon Inspector, especifique `"Resource": "*"` na política.

Chaves de condição do Amazon Inspector

O Inspector não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para Amazon Inspecto2

O Amazon Inspecto2 (prefixo do serviço: `inspector2`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Inspector2
- Tipos de recursos definidos pelo Amazon Inspector2
- Chaves de condição do Amazon Inspector2

Ações definidas pelo Amazon Inspector2

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateMember	Concede permissão para associar uma conta a uma conta de administrador do Amazon Inspector	Gravar			
BatchAssociateCodeSecurityScanConfiguration	Concede permissão para associar vários repositórios de código a uma configuração de verificação de segurança de código do Amazon Inspector	Gravar			
BatchDisassociateCodeSecurityScanConfiguration	Concede permissão para desassociar vários repositórios de código de uma configuração de verificação de segurança de código do Amazon Inspector	Gravar			
BatchGetAccountStatus	Concede permissão para recuperar informações sobre as contas do Amazon Inspector para uma conta	Leitura			
BatchGetCodeSnippet	Concede permissão para recuperar informações de trecho de código sobre uma ou mais descobertas de vulnerabilidade	Leitura			
BatchGetFindingDetails	Concede permissão para permitir que um cliente obtenha detalhes aprimorad	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	os de inteligência de vulnerabilidade para descobertas				
BatchGetFreeTrialInfo	Concede permissão para recuperar a elegibilidade do período de teste gratuito sobre contas do Amazon Inspector de uma conta	Leitura			
BatchGetMemberEc2DeepInspectionStatus	Concede permissão ao administrador delegado para recuperar o status de inspeção profunda do ec2 das contas-membros	Leitura			
BatchUpdateMemberEc2DeepInspectionStatus	Concede permissão para atualizar o status da inspeção profunda do ec2 pelo administrador delegado a suas contas-membros associadas	Gravar			
CancelFindingsReport	Concede permissão para cancelar a geração de um relatório de descobertas	Gravar			
CancelSbomExport	Concede permissão para cancelar a geração de um relatório SBOM	Gravar			
CreateCisScanConfiguration	Concede permissão para criar e definir as configurações de uma verificação do CIS	Gravar	CIS Scan Configuration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateCodeSecurityIntegration	Concede permissão para criar uma integração de segurança de código com um provedor de repositório de código-fonte	Gravar	Code Security Integration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCodeSecurityScanConfiguration	Concede permissão para criar uma configuração de escaneamento para escaneamento de segurança de código	Gravar	Code Security Scan Configuration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFilter	Concede permissão para criar e definir as configurações de um filtro de descobertas	Gravar	Filter*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFindingsReport	Concede permissão para solicitar a geração de um relatório de descobertas	Gravar			
CreateSbomExport	Concede permissão para solicitar a geração de um relatório SBOM	Gravar			
DeleteCisScanConfiguration	Concede permissão para excluir uma configuração de verificação do CIS	Gravar	CIS Scan Configuration*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteCodeSecurityIntegration	Concede permissão para excluir uma integração de segurança de código	Gravar	CodeSecurityIntegration*		
DeleteCodeSecurityScanConfiguration	Concede permissão para excluir uma configuração de verificação de segurança de código	Gravar	CodeSecurityScanConfiguration*		
DeleteFilter	Concede permissão para excluir um filtro de descobertas	Gravar	Filter*		
DescribeOrganizationConfiguration	Concede permissão para recuperar informações sobre as configurações do Amazon Inspector para uma organização AWS	Leitura			
Disable	Concede permissão para desabilitar uma conta do Amazon Inspector	Gravar			
DisableDelegatedAdminAccount	Concede permissão para desativar uma conta como conta de administrador delegado do Amazon Inspector para uma organização AWS	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateMember	Concede permissão para uma conta de administrador do Amazon Inspector para se desassociar de uma conta-membro do Inspector	Gravar			
Enable	Concede permissão para habilitar e especificar as configurações de uma nova conta do Amazon Inspector	Gravar			
EnableDelegatedAdminAccount	Concede permissão para habilitar uma conta como conta de administrador delegado do Amazon Inspector para uma organização AWS	Gravar			
GetCisScanReport	Concede permissão para recuperar um relatório contendo informações sobre verificações do CIS concluídas	Leitura			
GetCisScanResultDetails	Concede permissão para recuperar informações sobre todos os detalhes relacionados a uma verificação do CIS e um recurso de destino	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetClusterForImage	Concede permissão para obter informações de cluster para uma determinada imagem Amazon Ecr digitalizada continuamente	Leitura			
GetCodeSecurityIntegration	Concede permissão para recuperar informações sobre uma integração de segurança de código	Leitura			
GetCodeSecurityScan	Concede permissão para recuperar informações sobre uma verificação de segurança de código específica	Leitura			
GetCodeSecurityScanConfiguration	Concede permissão para recuperar informações sobre uma configuração de verificação de segurança de código	Leitura			
GetConfiguration	Concede permissão para recuperar informações sobre as configurações do Amazon Inspector para um Conta da AWS	Leitura			
GetDelegatedAdminAccount	Concede permissão para recuperar informações sobre a conta de administrador do Amazon Inspector para uma conta	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetEc2DeepInspectionConfiguration	Concede permissão para recuperar a configuração da inspeção profunda do ec2 a contas independentes, ao administrador delegado e a contas-membros	Leitura			
GetEncryptionKey	Concede permissão para recuperar informações sobre a chave do KMS usada para criptografar trechos de código com	Leitura			
GetFindingsReportStatus	Concede permissão para recuperar o status de um relatório de descobertas solicitado	Leitura			
GetMember	Concede permissão para recuperar informações sobre uma conta associada a uma conta de administrador do Amazon Inspector	Leitura			
GetSbomExport	Concede permissão para recuperar um relatório SBOM solicitado	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAccountPermissions	Concede permissão para recuperar permissões de configuração de recursos associadas a uma conta do Amazon Inspector em uma organização	Lista			
ListCisScanConfigurations	Concede permissão para recuperar informações sobre todas as configurações de verificação do CIS	Lista			
ListCisScanResultsAggregatedByChecks	Concede permissão para recuperar informações sobre todas as verificações relacionadas a uma verificação do CIS	Lista			
ListCisScanResultsAggregatedByTargetResource	Concede permissão para recuperar informações sobre todos os recursos relacionados a uma verificação do CIS	Lista			
ListCisScans	Concede permissão para recuperar informações sobre verificações do CIS concluídas	Lista			
ListCodeSecurityIntegrations	Concede permissão para listar todas as integrações de segurança de código em sua conta	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListCodeSecurityScanConfigurationAssociations	Concede permissão para listar as associações entre repositórios de código e configurações de verificação de segurança de código do Amazon Inspector	Lista			
ListCodeSecurityScanConfigurations	Concede permissão para listar todas as configurações de verificação de segurança de código em sua conta	Lista			
ListCoverage	Concede permissão para recuperar os tipos de estatísticas que o Amazon Inspector pode gerar para recursos monitores do Inspector	Lista			
ListCoverageStatistics	Concede permissão para recuperar dados estatísticos e outras informações sobre os recursos que o Amazon Inspector monitora	Lista			
ListDelegatedAdminAccounts	Concede permissão para recuperar informações sobre a conta de administrador delegada do Amazon Inspector para uma organização AWS	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListFilters	Concede permissão para recuperar informações sobre todos os filtros de descobertas	Lista			
ListFindingAggregations	Concede permissão para recuperar dados estatísticos e outras informações sobre descobertas do Amazon Inspector	Lista			
ListFindings	Concede permissão para recuperar um subconjunto de informações sobre uma ou mais descobertas	Lista			
ListMembers	Concede permissão para recuperar informações sobre as contas-membro do Amazon Inspector que estão associadas a uma conta de administrador do Inspector	Lista			
ListTagsForResource	Concede permissão para recuperar as etiquetas de um recurso do Amazon Inspector	Leitura			
ListUsageTotals	Concede permissão para recuperar dados de uso agregados de uma conta	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ResetEncryptionKey	Concede permissão para permitir que um cliente reinicie para usar uma chave KMS de propriedade da Amazon para criptografar trechos de código com	Gravar			
SearchVulnerabilities	Concede permissão para listar detalhes de cobertura do Amazon Inspector para uma vulnerabilidade específica	Leitura			
SendCisSessionHealth	Concede permissão para enviar a integridade do CIS para uma verificação do CIS	Gravar			
SendCisSessionTelemetry	Concede permissão para enviar telemetria do CIS para uma verificação do CIS	Gravar			
StartCisSession	Concede permissão para iniciar uma sessão de verificação do CIS	Gravar			
StartCodeSecurityScan	Concede permissão para iniciar uma verificação de segurança de código em um repositório especificado	Gravar			
StopCisSession	Concede permissão para interromper uma sessão de verificação do CIS	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para adicionar ou atualizar as etiquetas de um recurso do Amazon Inspector	Tags	CIS Scan Configuration		
			Code Security Integration		
			Code Security Scan Configuration		
			Filter		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
UntagResource	Concede permissão para remover etiquetas de um recurso do Amazon Inspector	Tags	CIS Scan Configuration		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			Code Security Integration		
			Code Security Scan Configuration		
			Filter		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCisScanConfiguration	Concede permissão para atualizar as definições de uma configuração de verificação do CIS	Gravar	CIS Scan Configuration*		
				aws:ResourceTag/${TagKey}	
UpdateCodeSecurityIntegration	Concede permissão para atualizar uma integração de segurança de código existente	Gravar	Code Security Integration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
UpdateCodeSecurityScanConfiguration	Concede permissão para atualizar uma configuração de verificação de segurança de código existente	Gravar	Code Security Scan Configuration*		
				aws:ResourceTag/${TagKey}	
UpdateConfiguration	Concede permissão para atualizar informações sobre as configurações do Amazon Inspector para um Conta da AWS	Gravar			
UpdateEc2DeepInspectionConfiguration	Concede permissão para atualizar a configuração da inspeção profunda do ec2 pelo administrador delegado e contas-membros e independentes	Gravar			
UpdateEncryptionKey	Concede permissão para permitir que um cliente use uma chave do KMS para criptografar trechos de código com	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateFilter	Concede permissão para atualizar as configurações de um filtro de descobertas	Gravar	Filter*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateOrgEc2DeepInspectionConfiguration	Concede permissão para atualizar a configuração da inspeção profunda do ec2 pelo administrador delegado a suas contas-membros associadas	Gravar			
UpdateOrganizationConfiguration	Concede permissão para atualizar as configurações do Amazon Inspector para uma organização AWS	Gravar			

Tipos de recursos definidos pelo Amazon Inspector2

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
Filter	`arn:${Partition}:inspector2:${Region}:${Account}:owner/${OwnerId}/filter/${FilterId}`	aws:ResourceTag/${TagKey}
Finding	`arn:${Partition}:inspector2:${Region}:${Account}:finding/${FindingId}`	
CIS Scan Configuration	`arn:${Partition}:inspector2:${Region}:${Account}:owner/${OwnerId}/cis-configuration/${CISScanConfigurationId}`	aws:ResourceTag/${TagKey}
Code Security Scan Configuration	`arn:${Partition}:inspector2:${Region}:${Account}:owner/${OwnerId}/codesecurity-configuration/${CodeSecurityScanConfigurationId}`	aws:ResourceTag/${TagKey}
Code Security Integration	`arn:${Partition}:inspector2:${Region}:${Account}:codesecurity-integration/${CodeSecurityIntegrationId}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Inspector2

O Amazon Inspector2 define as chaves de condição a seguir que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para a Amazon InspectorScan

A Amazon InspectorScan (prefixo do serviço:`inspector-scan`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon InspectorScan
- Tipos de recursos definidos pela Amazon InspectorScan
- Chaves de condição para a Amazon InspectorScan

Ações definidas pela Amazon InspectorScan

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou

ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ScanSbom	Concede permissão para examinar o SBOM fornecido pelo cliente e retornar vulnerabilidades nele detectadas	Leitura			

Tipos de recursos definidos pela Amazon InspectorScan

InspectorScan A Amazon não suporta a especificação de um ARN de recurso no elemento de uma `Resource` declaração de política do IAM. Para permitir o acesso à Amazon InspectorScan, especifique `"Resource": "*"` em sua política.

Chaves de condição para a Amazon InspectorScan

InspectorScan não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do Amazon Interactive Video Service

O Amazon Interactive Video Service (prefixo do serviço: `ivs`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Interactive Video Service
- Tipos de recursos definidos pelo Amazon Interactive Video Service
- Chaves de condição do Amazon Interactive Video Service

Ações definidas pelo Amazon Interactive Video Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de

recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchGetChannel	Concede permissão para obter vários canais simultaneamente pelo ARN do canal	Leitura	Channel*		
BatchGetStreamKey	Concede permissão para obter várias chaves de stream simultaneamente pelo ARN da chave de stream	Leitura	Stream-Key*		
BatchStartViewerSessionRevocation	Concede permissão para atuar StartViewerSessionRevocation em vários pares de ARN e ID de visualizador de canais simultaneamente	Gravar	Channel*		
CreateChannel	Concede permissão para criar um canal e uma chave de stream associada	Gravar	Channel*		
			Stream-Key*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateEncoderConfiguration	Concede permissão para criar uma nova configuração de codificador	Gravar	Encoder-Configuration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateIngestConfiguration	Concede permissão para criar uma configuração de ingestão	Gravar	Ingest-Configuration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateParticipantToken	Concede permissão para criar um token de participante	Gravar	Stage*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreatePlaybackRestrictionPolicy	Concede permissão para criar uma política de restrição de reprodução	Gravar	Playback-Restriction-Policy*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateRecordingConfiguration	Concede permissão para criar uma nova configuração de gravação	Gravar	Recording-Configuration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStage	Concede permissão para criar um estágio	Gravar	Stage*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateStorageConfiguration	Concede permissão para criar uma nova configuração de armazenamento	Gravar	Storage-Configuration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStreamKey	Concede permissão para criar uma chave de stream	Gravação	Stream-Key*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteChannel	Concede permissão para excluir um canal e as chaves de stream do canal	Gravar	Channel*		
			Stream-Key*		
DeleteEncoderConfiguration	Concede permissão para excluir uma configuração de codificador para o ARN especificado	Gravar	Encoder-Configuration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteIngestConfiguration	Concede permissão para excluir uma configuração de ingestão do ARN especificado	Gravar	Ingest-Configuration*		
DeletePlaybackKeyPair	Concede permissão para excluir o par de chaves de reprodução de um ARN especificado	Gravar	Playback-Key-Pair*		
DeletePlaybackRestrictionPolicy	Concede permissão para excluir a política de restrição de reprodução de um ARN especificado	Gravar	Playback-Restriction-Policy*		
DeletePublicKey	Concede permissão para excluir a chave pública do ARN especificado	Gravar	Public-Key*		
DeleteRecordingConfiguration	Concede permissão para excluir uma configuração de gravação para o ARN especificado	Gravar	Recording-Configuration*		
DeleteStage	Concede permissão para excluir o estágio de um ARN especificado	Gravar	Stage*		
DeleteStorageConfiguration	Concede permissão para excluir uma configuração de armazenamento para o ARN especificado	Gravar	Storage-Configuration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteStreamKey	Concede permissão para excluir a chave de stream de um ARN especificado	Gravar	Stream-Key*		
DisconnectParticipant	Concede permissão para desconectar um participante do ARN de estágio especificado	Gravar	Stage*		
GetChannel	Concede permissão para obter a configuração do canal para o ARN de um canal especificado	Leitura	Channel*		
GetComposition	Concede permissão para obter a composição para o ARN especificado	Leitura	Composition*		
GetEncoderConfiguration	Concede permissão para obter a configuração do codificador para o ARN especificado	Leitura	Encoder-Configuration*		
GetIngestConfiguration	Concede permissão para obter a configuração de ingestão do ARN especificado	Leitura	Ingest-Configuration*		
GetParticipant	Concede permissão para obter informações de participante de um participante, sessão e ARN de estágio especificado	Leitura	Stage*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetPlaybackKeyPair	Concede permissão para obter as informações do par de chaves de reprodução de um ARN especificado	Leitura	Playback-Key-Pair*		
GetPlaybackRestrictionPolicy	Concede permissão para obter a política de restrição de reprodução para um ARN especificado	Leitura	Playback-Restriction-Policy*		
GetPublicKey	Concede permissão para obter a chave pública do ARN especificado	Leitura	Public-Key*		
GetRecordingConfiguration	Concede permissão para obter a configuração de gravação para o ARN especificado	Leitura	Recording-Configuration*		
GetStage	Concede permissão para obter informações de estágio para um ARN especificado	Leitura	Stage*		
GetStageSession	Concede permissão para obter informações de sessão de estágio de uma sessão e um ARN de estágio especificado	Leitura	Stage*		
GetStorageConfiguration	Concede permissão para obter a configuração de armazenamento para o ARN especificado	Leitura	Storage-Configuration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetStream	Concede permissão para obter informações sobre o stream ativo (ao vivo) em um canal especificado	Leitura	Channel*		
GetStreamKey	Concede permissão para obter informações de chave de stream para um ARN especificado	Leitura	Stream-Key*		
GetStreamSession	Concede permissão para obter informações sobre a sessão de transmissão em um canal especificado	Leitura	Channel*		
ImportPlaybackKeyPair	Concede permissão para importar a chave pública	Gravar	Playback-Key-Pair*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ImportPublicKey	Concede permissão para importar uma chave pública	Gravar	Public-Key*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListChannels	Concede permissão para obter informações resumidas sobre canais	Lista	Channel*		
ListCompositions	Concede permissão para obter informações de resumo sobre composições	Lista	Encoder-Configuration		
			Stage		
ListEncoderConfigurations	Concede permissão para obter informações de resumo sobre configurações de codificador	Lista			
ListIngestConfigurations	Concede permissão para obter informações de resumo sobre configurações de ingestão	Lista			
ListParticipantEvents	Concede permissão para listar eventos de participante de um participante, sessão e ARN de estágio especificado	Lista	Stage*		
ListParticipantReplicas	Concede permissão para obter informações resumidas sobre as réplicas dos participantes	Lista	Stage*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListParticipants	Concede permissão para listar participantes de uma sessão e ARN de estágio especificado	Lista	Stage*		
ListPlaybackKeyPairs	Concede permissão para obter informações resumidas sobre pares de chaves de reprodução	Lista	Playback-Key-Pair*		
ListPlaybackRestrictionPolicies	Concede permissão para obter informações resumidas sobre políticas de restrição de reprodução	Lista			
ListPublicKeys	Concede permissão para obter informações resumidas sobre chaves públicas	Lista			
ListRecordingConfigurations	Concede permissão para obter informações de resumo sobre configurações de gravação	Lista	Recording-Configuration*		
ListStageSessions	Concede permissão para listar sessões de um ARN de estágio especificado	Lista	Stage*		
ListStages	Concede permissão para obter informações resumidas sobre estágios	Lista	Stage*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListStorageConfigurations	Concede permissão para obter informações de resumo sobre configurações de armazenamento	Lista			
ListStreamKeys	Concede permissão para obter informações resumidas sobre chaves de stream	Lista	Channel*		
			Stream-Key*		
ListStreamSessions	Concede permissão para obter informações de resumo sobre as sessões de transmissão em canal especificado	Lista	Channel*		
ListStreams	Concede permissão para obter informações resumidas sobre streams ao vivo	List	Channel*		
ListTagsForResource	Concede permissão para obter informações sobre as etiquetas de um ARN especificado	Leitura	Channel		
			Composition		
			Encoder-Configuration		
			Ingest-Configuration		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			Playback-Key-Pair		
			Playback-Restriction-Policy		
			Public-Key		
			Recording-Configuration		
			Stage		
			Storage-Configuration		
			Stream-Key		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutMetadata	Concede permissão para inserir metadados em um stream RTMP para um canal especificado	Gravar	Channel*		
StartComposition	Concede permissão para iniciar uma nova composição	Gravar	Encoder-Configuration*		
			Stage*		
			Channel		
			Storage-Configuration		
				aws:TagKeys aws:RequestTag/${TagKey}	
StartParticipantReplication	Concede permissão para iniciar uma nova replicação de participantes	Gravar	Stage*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartViewerSessionRevocation	Concede permissão para iniciar o processo de revogação da sessão do visualizador associada a um ARN de canal e ID do visualizador especificados	Gravar	Channel*		
StopComposition	Concede permissão para interromper a composição para o ARN especificado	Gravar	Composition*		
StopParticipantReplication	Concede permissão para interromper a replicação do participante para o ARN especificado	Gravar	Stage*		
StopStream	Concede permissão para desconectar um streamer em um canal especificado	Gravação	Channel*		
TagResource	Concede permissão para adicionar ou atualizar etiquetas para um recurso com um ARN especificado	Marcação	Channel		
			Composition		
			Encoder-Configuration		
			Ingest-Configuration		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			Playback-Key-Pair		
			Playback-Restriction-Policy		
			Public-Key		
			Recording-Configuration		
			Stage		
			Storage-Configuration		
			Stream-Key		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para remover etiquetas de um recurso com um ARN especificado	Marcação	Channel		
			Composition		
			Encoder-Configuration		
			Ingest-Configuration		
			Playback-Key-Pair		
			Playback-Restriction-Policy		
			Public-Key		
			Recording-Configuration		
			Stage		
			Storage-Configuration		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			Stream-Key		
				aws:TagKeys	
UpdateChannel	Concede permissão para atualizar a configuração de um canal	Gravar	Channel*		
UpdateIngestConfiguration	Concede permissão para atualizar a configuração de ingestão de um ARN especificado	Gravar	Ingest-Configuration*		
UpdatePlaybackRestrictionPolicy	Concede permissão para atualizar uma política de restrição de reprodução para um ARN especificado	Gravar	Playback-Restriction-Policy*		
UpdateStage	Concede permissão para atualizar a configuração de um estágio	Gravar	Stage*		

Tipos de recursos definidos pelo Amazon Interactive Video Service

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}
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}

Tipos de recursos	ARN	Chaves de condição
Ingest-Configuration	`arn:${Partition}:ivs:${Region}:${Account}:ingest-configuration/${ResourceId}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Interactive Video Service

O Amazon Interactive Video Service define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas associadas com a solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do chat do Amazon Interactive Video Service

Chat do Amazon Interactive Video Service (prefixo do serviço: `ivschat`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo chat do Amazon Interactive Video Service
- Tipos de recursos definidos pelo chat do Amazon Interactive Video Service
- Chaves de condição para o chat do Amazon Interactive Video Service

Ações definidas pelo chat do Amazon Interactive Video Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateChatToken	Concede permissão para criar um token criptografado que é usado para estabelecer uma WebSocket conexão individual com uma sala	Gravar	Room*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateLoggingConfiguration	Concede permissão para criar uma configuração de log que permite que os clientes registrem mensagens da sala	Gravar	Logging-Configuration*		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey}	
CreateRoom	Concede permissão para criar uma sala que permite que os clientes se conectem e transmitam mensagens	Gravar	Room*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteLoggingConfiguration	Concede permissão para excluir a configuração de log para um ARN de configuração de log especificado	Gravar	Logging-Configuration*		
DeleteMessage	Concede permissão para enviar um evento para uma sala específica que direciona os clientes a excluir uma mensagem específica	Gravar	Room*		
DeleteRoom	Concede permissão para excluir a a sala de um ARN especificado	Gravar	Room*		
DisconnectUser	Concede permissão para desconectar todas as conexões usando um ID de usuário especificado de uma sala	Gravar	Room*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetLoggingConfiguration	Concede permissão para obter a configuração de log para um ARN de configuração de log especificado	Leitura	Logging-Configuration*		
GetRoom	Concede permissão para obter a configuração da sala para o ARN de uma sala especificada	Leitura	Room*		
ListLoggingConfigurations	Concede permissão para obter informações de resumo sobre configurações de log	Lista	Logging-Configuration*		
ListRooms	Concede permissão para obter informações resumidas sobre salas	Lista	Room*		
ListTagsForResource	Concede permissão para obter informações sobre as etiquetas de um ARN especificado	Leitura	Room		
				aws:TagKeys aws:RequestTag/${TagKey}	
SendEvent	Concede permissão para enviar um evento a uma sala	Gravar	Room*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para adicionar ou atualizar etiquetas para um recurso com um ARN especificado	Marcação	Logging-Configuration		
			Room		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover etiquetas de um recurso com um ARN especificado	Tags	Logging-Configuration		
			Room		
				aws:TagKeys	
UpdateLoggingConfiguration	Concede permissão para atualizar a configuração de log para um ARN de configuração de log especificado	Gravar	Logging-Configuration*		
UpdateRoom	Concede permissão para atualizar a configuração da sala para o ARN de uma sala especificada	Gravar	Room*		

Tipos de recursos definidos pelo chat do Amazon Interactive Video Service

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
Room	`arn:${Partition}:ivschat:${Region}:${Account}:room/${ResourceId}`	aws:ResourceTag/${TagKey}
Logging-Configuration	`arn:${Partition}:ivschat:${Region}:${Account}:logging-configuration/${ResourceId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o chat do Amazon Interactive Video Service

O chat do Amazon Interactive Video Service define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas associadas com a solicitação	Segmento

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS Invoicing Service

AWS O Invoicing Service (prefixo do serviço:`invoicing`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Invoicing Service
- Tipos de recursos definidos pelo AWS Invoicing Service
- Chaves de condição para o AWS Invoicing Service

Ações definidas pelo AWS Invoicing Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchGetInvoiceProfile	Concede permissão para obter detalhes do perfil da fatura de uma conta na sua organização	Leitura			
CreateInvoiceUnit	Concede permissão para criar uma unidade de fatura para sua organização	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteInvoiceUnit	Concede permissão para atualizar uma unidade de fatura para sua organização	Gravar	invoice-unit*		
				aws:ResourceTag/${TagKey}	
GetInvoiceEmailDeliveryPreferences [somente permissão]	Concede permissão para obter preferências de entrega de e-mail de fatura	Leitura			
GetInvoicePDF [somente permissão]	Concede permissão para obter permissão para um PDF de fatura	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetInvoiceUnit	Concede permissão para obter unidades de fatura para sua organização	Leitura	invoice-unit*		
ListInvoiceSummaries	Concede permissão para obter informações resumidas da fatura para sua conta ou para uma conta vinculada	Leitura			
ListInvoiceUnits	Concede permissão para listar unidades de fatura para sua organização	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	invoice-unit*		
				aws:ResourceTag/${TagKey}	
PutInvoiceEmailDeliveryPreferences [somente permissão]	Concede permissão para inserir preferências de entrega de e-mail de fatura	Gravar			
TagResource	Concede permissão para marcar um recurso	Marcação	invoice-unit*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permissão para desmarcar um recurso	Tags	invoice-unit*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateInvoiceUnit	Concede permissão para atualizar uma unidade de fatura para sua organização	Gravar	invoice-unit*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pelo AWS Invoicing Service

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso

também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
invoice-unit	`arn:${Partition}:invoicing::${Account}:invoice-unit/${Identifier}`	aws:ResourceTag/${TagKey}

Chaves de condição para o AWS Invoicing Service

AWS O Invoicing Service define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por conjunto de valores permitido para cada uma das etiquetas	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelo valor-etiqueta associado ao recurso	String
aws:TagKeys	Filtra o acesso por presença de etiquetas obrigatórias na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS IoT 1-Click

AWS O IoT 1-Click (prefixo do serviço`iot1click`:) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS IoT 1-Click
- Tipos de recursos definidos pelo AWS IoT 1-Click
- Chaves de condição do AWS IoT 1-Click

Ações definidas pelo AWS IoT 1-Click

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateDeviceWithPlacement	Concede permissão para associar um dispositivo a um posicionamento	Write	project*		
ClaimDevicesByClaimCode	Concede permissão para reivindicar um lote de dispositivos com um código de reivindicação	Read			
CreatePlacement	Concede permissão para criar um novo posicionamento em um projeto	Write	project*		
CreateProject	Concede permissão para criar um novo projeto	Write	project*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeletePlacement	Concede permissão para excluir um posicionamento de um projeto	Write	project*		
DeleteProject	Concede permissão para excluir um projeto	Write	project*		
DescribeDevice	Concede permissão para descrever um dispositivo	Read	device*		
DescribePlacement	Concede permissão para descrever um posicionamento	Read	project*		
DescribeProject	Concede permissão para descrever um projeto	Read	project*		
DisassociateDeviceFromPlacement	Concede permissão para desassociar um dispositivo de um posicionamento	Write	project*		
FinalizeDeviceClaim	Concede permissão para finalizar a reivindicação de um dispositivo	Read	device*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
GetDeviceMethods	Concede permissão para obter métodos disponíveis de um dispositivo	Read	device*		
GetDevicesInPlacement	Concede permissão para obter dispositivos associados a um posicionamento	Read	project*		
InitiateDeviceClaim	Concede permissão para inicializar uma reivindicação de dispositivo	Read	device*		
InvokeDeviceMethod	Concede permissão para invocar um método de dispositivo	Write	device*		
ListDeviceEvents	Concede permissão para listar eventos passados publicados por um dispositivo	Read	device*		
ListDevices	Concede permissão para listar todos os dispositivos	List			
ListPlacements	Concede permissão para listar posicionamentos em um projeto	Read	project*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListProjects	Concede permissão para listar todos os projetos	List			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Read	device		
			project		
TagResource	Concede permissão para adicionar ou modificar as etiquetas de um recurso	Marcação	device		
			project		
				aws:RequestTag/${TagKey} aws:TagKeys	
UnclaimDevice	Concede permissão para cancelar a reivindicação de um dispositivo	Read	device*		
UntagResource	Concede permissão para remover as etiquetas fornecidas (metadados) de um recurso	Marcação	device		
			project		
				aws:TagKeys	
UpdateDeviceState	Concede permissão para atualizar o estado do dispositivo	Write	device*		
UpdatePlacement	Concede permissão para atualizar um posicionamento	Write	project*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateProject	Atualizar um projeto	Write	project*		

Tipos de recursos definidos pelo AWS IoT 1-Click

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
device	`arn:${Partition}:iot1click:${Region}:${Account}:devices/${DeviceId}`	aws:ResourceTag/${TagKey}
project	`arn:${Partition}:iot1click:${Region}:${Account}:projects/${ProjectName}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS IoT 1-Click

AWS O IoT 1-Click define as seguintes chaves de condição que podem ser usadas no elemento de uma `Condition` política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra ações com base nas etiquetas transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra as ações com base nas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra ações com base nas chaves da etiqueta transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS IoT Analytics

AWS O IoT Analytics (prefixo do serviço`iotanalytics`:) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS IoT Analytics
- Tipos de recursos definidos pelo AWS IoT Analytics
- Chaves de condição do AWS IoT Analytics

Ações definidas pelo AWS IoT Analytics

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchPutMessage	Coloca um lote de mensagens no canal especificado	Gravar	channel*		
CancelPipelineReprocessing	Cancela o reprocessamento do pipeline especificado	Gravar	pipeline*		
CreateChannel	Cria um canal	Gravar	channel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataset	Cria um conjunto de dados	Gravar	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDatasetContent	Gera o conteúdo do conjunto de dados especificado (executando as ações do conjunto de dados)	Gravar	dataset*		
CreateDatastore	Cria um datastore	Gravar	datastore*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePipeline	Cria um pipeline	Gravar	pipeline*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Exclui o canal especificado	Gravar	channel*		
DeleteDataset	Exclui o conjunto de dados especificado	Gravar	dataset*		
DeleteDatasetContent	Exclui o conteúdo do conjunto de dados especificado	Gravar	dataset*		
DeleteDatastore	Exclui o datastore especificado	Gravar	datastore*		
DeletePipeline	Exclui o pipeline especificado	Gravar	pipeline*		
DescribeChannel	Descreve o canal especificado	Leitura	channel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeDataset	Descreve o conjunto de dados especificado	Leitura	dataset*		
DescribeDatastore	Descreve o datastore especificado	Leitura	datastore*		
DescribeLoggingOptions	Descreve as opções de log da conta	Leitura			
DescribePipeline	Descreve o pipeline especificado	Leitura	pipeline*		
GetDatasetContent	Obtém o conteúdo do conjunto de dados especificado	Leitura	dataset*		
ListChannels	Lista os canais da conta	Lista			
ListDatasetContents	Lista informações sobre o conteúdo do conjunto de dados que foi criado	Lista	dataset*		
ListDatasets	Lista os conjuntos de dados da conta	Lista			
ListDatastores	Lista os datastores da conta	Lista			
ListPipelines	Lista os pipelines da conta	Lista			
ListTagsForResource	Lista as etiquetas (metadados) que você atribuiu ao recurso	Leitura	channel		
			dataset		
			datastore		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			pipeline		
PutLoggingOptions	Coloca as opções de log da conta	Gravar			
RunPipelineActivity	Executa a atividade do pipeline especificado	Leitura			
SampleChannelData	Amostra os dados do canal especificado	Leitura	channel*		
StartPipelineReprocessing	Inicia o reprocessamento do pipeline especificado	Gravar	pipeline*		
TagResource	Adiciona ou modifica as etiquetas do determinado recurso. Etiquetas são metadados que podem ser usados para gerenciar um recurso	Tags	channel		
			dataset		
			datastore		
			pipeline		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Remove as etiquetas determinadas (metadados) do recurso	Tags	channel		
			dataset		
			datastore		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			pipeline		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateChannel	Atualiza o canal especificado	Gravar	channel*		
UpdateDataset	Atualiza o conjunto de dados especificado	Gravar	dataset*		
UpdateDatastore	Atualiza o datastore especificado	Gravar	datastore*		
UpdatePipeline	Atualiza o pipeline especificado	Gravar	pipeline*		

Tipos de recursos definidos pelo AWS IoT Analytics

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS IoT Analytics

AWS O IoT Analytics define as seguintes chaves de condição que podem ser usadas `Condition` no elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições

sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base nas etiquetas transmitidas na solicitação	String
aws:TagKeys	Filtra o acesso com base na presença de chaves da etiqueta na solicitação	ArrayOfString
iotanalytics:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String

Ações, recursos e chaves de condição do AWS IoT Core Device Advisor

AWS O IoT Core Device Advisor (prefixo do serviço:`iotdeviceadvisor`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS IoT Core Device Advisor
- Tipos de recursos definidos pelo AWS IoT Core Device Advisor
- Chaves de condição para o AWS IoT Core Device Advisor

Ações definidas pelo AWS IoT Core Device Advisor

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSuiteDefinition	Concede permissão para criar uma definição de suíte	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSuiteDefinition	Concede permissão para excluir uma definição de suíte	Gravar	Suitedefinition*		
GetEndpoint	Concede permissão para obter um endpoint do Device Advisor	Leitura			
GetSuiteDefinition	Concede permissão para obter uma definição de suíte	Read	Suitedefinition*		
GetSuiteRun	Concede permissão para executar uma suíte	Read	Suiterun*		
GetSuiteRunReport	Concede permissão para obter o relatório de qualificação para uma execução de suíte	Read	Suiterun*		
ListSuiteDefinitions	Concede permissão para listar definições de suíte	List			
ListSuiteRuns	Concede permissão para listar execuções de suíte	List	Suitedefinition*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar as etiquetas (metadados) atribuídas a um recurso	Read	Suitedefinition		
			Suiterun		
StartSuiteRun	Concede permissão para iniciar uma execução de suíte	Write		aws:RequestTag/${TagKey} aws:TagKeys	
StopSuiteRun	Concede permissão para interromper a execução de um conjunto.	Write	Suiterun*		
TagResource	Concede permissão para adicionar ou modificar as etiquetas do recurso fornecido. Etiquetas são metadados que podem ser usados para gerenciar um recurso	Marcação	Suitedefinition		
			Suiterun		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover as etiquetas fornecidas (metadados) de um recurso	Marcação	Suitedefinition		
			Suiterun		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
UpdateSuiteDefinition	Concede permissão para atualizar uma definição de suíte	Write	Suitedefinition*		

Tipos de recursos definidos pelo AWS IoT Core Device Advisor

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
Suitedefinition	`arn:${Partition}:iotdeviceadvisor:${Region}:${Account}:suitedefinition/${SuiteDefinitionId}`	aws:ResourceTag/${TagKey}
Suiterun	`arn:${Partition}:iotdeviceadvisor:${Region}:${Account}:suiterun/${SuiteDefinitionId}/${SuiteRunId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o AWS IoT Core Device Advisor

AWS O IoT Core Device Advisor define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais

as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS IoT Device Tester

AWS O IoT Device Tester (prefixo do serviço:`iot-device-tester`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS IoT Device Tester
- Tipos de recursos definidos pelo AWS IoT Device Tester
- Chaves de condição do AWS IoT Device Tester

Ações definidas pelo AWS IoT Device Tester

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CheckVersion	Concede permissão para o IoT Device Tester verificar se uma determinada definição de produto, conjunto de testes e versão do testador de dispositivos são compatíveis	Leitura			
DownloadTestSuite	Concede permissão para o IoT Device Tester fazer download de versões compatíveis do conjunto de testes	Leitura			
LatestIdt	Concede permissão ao IoT Device Tester para obter informações sobre a versão mais recente do testador de dispositivos disponível	Leitura			
SendMetrics	Concede permissões ao IoT Device Tester para enviar métricas de uso em seu nome	Gravar			
SupportedVersion	Concede permissão para o IoT Device Tester para obter a lista de versões do conjunto de testes e produtos compatíveis	Leitura			

Tipos de recursos definidos pelo AWS IoT Device Tester

AWS O IoT Device Tester não suporta a especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para conceder acesso ao AWS IoT Device Tester, especifique `"Resource": "*"` na política.

Chaves de condição do AWS IoT Device Tester

O IoT Device Tester não tem chaves de contexto específicas ao serviço que possam ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS IoT Events

AWS O IoT Events (prefixo do serviço`iotevents`:) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS IoT Events
- Tipos de recursos definidos pelo AWS IoT Events
- Chaves de condição do AWS IoT Events

Ações definidas pelo AWS IoT Events

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchAcknowledgeAlarm	Concede permissão para enviar uma ou mais solicitações de ação de reconhecimento para a AWS IoT Events	Gravar	alarmModel*		
BatchDeleteDetector	Concede permissão para excluir uma instância do detector no sistema AWS IoT Events	Gravar	detectorModel*		
BatchDisableAlarm	Concede permissão para desativar uma ou mais instâncias de alarme	Write	alarmModel*		
BatchEnableAlarm	Concede permissão para habilitar uma ou mais instâncias de alarme	Gravar	alarmModel*		
BatchPutMessage	Concede permissão para enviar um conjunto de mensagens para o sistema AWS IoT Events	Gravar	input*		
BatchResetAlarm	Concede permissão para redefinir uma ou mais instâncias de alarme	Write	alarmModel*		
BatchSnoozeAlarm	Concede permissão para alterar uma ou mais instâncias de alarme para o modo soneca	Gravar	alarmModel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchUpdateDetector	Concede permissão para atualizar uma instância do detector no sistema AWS IoT Events	Gravar	detectorModel*		
CreateAlarmModel	Concede permissão para criar um modelo de alarme para monitorar um atributo de entrada de Eventos de AWS IoT ou uma propriedade de ativo de AWS IoT SiteWise	Gravar	alarmModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDetectorModel	Concede permissão para criar um modelo de detector para monitorar um atributo de AWS entrada do IoT Events	Gravar	detectorModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInput	Concede permissão para criar uma entrada no IotEvents	Gravar	input*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteAlarmModel	Concede permissão para excluir um modelo de alarme	Write	alarmModel*		
DeleteDetectorModel	Concede permissão para excluir um modelo de detector	Write	detectorModel*		
DeleteInput	Concede permissão para excluir uma entrada	Write	input*		
DescribeAlarm	Concede permissão para recuperar informações sobre uma instância de alarme	Read	alarmModel*		
DescribeAlarmModel	Concede permissão para recuperar informações sobre um modelo de alarme	Read	alarmModel*		
DescribeDetector	Concede permissão para recuperar informações sobre uma instância de detector	Read	detectorModel*		
DescribeDetectorModel	Concede permissão para recuperar informações sobre um modelo de detector	Leitura	detectorModel*		
DescribeDetectorModelAnalysis	Concede permissão para recuperar informações de análise do modelo de detector	Leitura			
DescribeInput	Concede permissão para recuperar informações sobre Entrada	Leitura	input*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeLoggingOptions	Concede permissão para recuperar as configurações atuais das opções de registro do AWS IoT Events	Leitura			
GetDetectorModelAnalysisResults	Concede permissão para recuperar resultados da análise do modelo de detector	Leitura			
ListAlarmModelVersions	Concede permissão para listar todas as versões de um modelo de alarme	List	alarmModel*		
ListAlarmModels	Concede permissão para listar os modelos de alarme que você criou	List			
ListAlarms	Concede permissão para recuperar informações sobre todas as instâncias de alarme por alarmModel	List	alarmModel*		
ListDetectorModelVersions	Concede permissão para listar todas as versões de um modelo de detector	List	detectorModel*		
ListDetectorModels	Concede permissão para listar os modelos de detector que você criou	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDetectors	Concede permissão para recuperar informações sobre todas as instâncias do detector por detectormodel	List	detectorModel*		
ListInputRoutings	Concede permissão para relacionar um ou mais roteamentos de entrada	List			
ListInputs	Concede permissão para lista as entradas que você criou	List			
ListTagsForResource	Concede permissão para listar as etiquetas (metadados) que você atribuiu ao recurso	Leitura	alarmModel		
			detectorModel		
			input		
PutLoggingOptions	Concede permissão para definir ou atualizar as opções de AWS registro do IoT Events	Gravar			
StartDetectorModelAnalysis	Concede permissão para iniciar a análise do modelo do detector	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para adicionar ou modificar as etiquetas do recurso indicado. Etiquetas são metadados que podem ser usados para gerenciar um recurso	Marcação	alarmModel		
			detectorModel		
			input		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover as etiquetas fornecidas (metadados) do recurso	Marcação	alarmModel		
			detectorModel		
			input		
				aws:TagKeys	
UpdateAlarmModel	Concede permissão para atualizar um modelo de alarme	Write	alarmModel*		
UpdateDetectorModel	Concede permissão para atualizar um modelo de detector	Write	detectorModel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateInput	Concede permissão para atualizar uma entrada	Write	input*		
UpdateInputRouting	Concede permissão para atualizar o roteamento de entrada	Write	input*		

Tipos de recursos definidos pelo AWS IoT Events

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS IoT Events

AWS O IoT Events define as seguintes chaves de condição que podem ser usadas `Condition` no elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso pelos pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas anexadas ao recurso	String
aws:TagKeys	Filtra ações pelas chaves da etiqueta na solicitação	ArrayOfString
iotevents:keyValue	Filtra o acesso pelo instanceId (chave-valor) da mensagem	String

Ações, recursos e chaves de condição do AWS IoT Fleet Hub for Device Management

AWS O IoT Fleet Hub para gerenciamento de dispositivos (prefixo do serviço:`iotfleethub`) fornece os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS IoT Fleet Hub for Device Management
- Tipos de recursos definidos pelo AWS IoT Fleet Hub for Device Management
- Chaves de condição para o AWS IoT Fleet Hub for Device Management

Ações definidas pelo AWS IoT Fleet Hub for Device Management

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateApplication	Concede permissão para criar um aplicativo	Write		aws:RequestTag/${TagKey} aws:TagKeys	sso:CreateManagedApplicationInstance sso:DescribeRegisteredRegions
DeleteApplication	Concede permissão para excluir um aplicativo	Write	application*		sso:DeleteManagedApplicationInstance
DescribeApplication	Concede permissão para descrever um ativo	Read	application*		
ListApplications	Concede permissão para listar todos as aplicações	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar todas as etiquetas de um recurso	Read	application		
TagResource	Concede permissão para marcar um recurso	Marcação	application		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para desmarcar um recurso	Marcação	application		
				aws:TagKeys	
UpdateApplication	Concede permissão para atualizar uma aplicação	Write	application*		

Tipos de recursos definidos pelo AWS IoT Fleet Hub for Device Management

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
application	`arn:${Partition}:iotfleethub:${Region}:${Account}:application/${ApplicationId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o AWS IoT Fleet Hub for Device Management

AWS O IoT Fleet Hub for Device Management define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso pelos pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas anexadas ao recurso	String
aws:TagKeys	Filtra ações pelas chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para AWS IoT FleetWise

AWS A IoT FleetWise (prefixo do serviço:`iotfleetwise`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.

- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela AWS IoT FleetWise
- Tipos de recursos definidos pela AWS IoT FleetWise
- Chaves de condição para AWS IoT FleetWise

Ações definidas pela AWS IoT FleetWise

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateVehicleFleet	Concede permissão para associar um determinado veículo a uma frota	Gravar	fleet*		
			vehicle*		
CreateCampaign	Concede permissão para criar uma campanha	Gravar	campaign*		
			fleet*		
			signalcatalog*		
			vehicle*		
				aws:RequestTag/${TagKey} aws:TagKeys iotfleetwise:DestinationArn	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDecoderManifest	Concede permissão para criar um manifesto de decodificador para um modelo existente	Gravar	decodermanifest*		
			modelmanifest*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFleet	Concede permissão para criar uma frota	Gravar	fleet*		
			signalcatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelManifest	Concede permissão para criar uma definição de trabalho de manifesto de modelo	Gravar	modelmanifest*		
			signalcatalog*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSignalCatalog	Concede permissão para criar um catálogo de sinalização	Gravar	signalcatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStateTemplate	Concede permissão para criar um modelo de estado	Gravar	signalcatalog*		
			statetemplate*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateVehicle	Concede permissão para criar um veículo	Gravar	decodermanifest*		iot:CreateThing iot:DescribeThing
			modelmanifest*		
			vehicle*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCampaign	Concede permissão para excluir uma campanha	Gravar	campaign*		
DeleteDecoderManifest	Concede permissão para excluir o manifesto do decodificador fornecido	Gravar	decodermanifest*		
DeleteFleet	Concede permissão para excluir uma frota	Gravar	fleet*		
DeleteModelManifest	Concede permissão para excluir o manifesto do modelo fornecido	Gravar	modelmanifest*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteSignalCatalog	Concede permissão para excluir um catálogo de sinal específico	Gravar	signalcatalog*		
DeleteStateTemplate	Concede permissão para excluir um modelo de estado	Gravar	statetemplate*		
DeleteVehicle	Concede permissão para excluir um veículo	Gravar	vehicle*		
DisassociateVehicleFleet	Concede permissão para desassociar um veículo de uma frota existente	Gravar	fleet*		
			vehicle*		
GenerateCommandPayload [somente permissão]	Concede permissão para gerar a carga útil para executar um comando em um veículo	Gerenciamento de permissões	vehicle*		
			statetemplate		
				iotfleetwise:Signals	
GetCampaign	Concede permissão para obter informações resumidas de uma determinada campanha	Leitura	campaign*		
GetDecoderManifest	Concede permissão para obter informações resumidas de uma determinada definição de manifesto de decodificador	Leitura	decodermanifest*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetEncryptionConfiguration	Concede permissão para obter o status de criptografia baseado em KMS para o Conta da AWS	Leitura			
GetFleet	Concede permissão para obter informações resumidas sobre uma frota	Leitura	fleet*		
GetLoggingOptions	Concede permissão para obter as opções de registro para o Conta da AWS	Leitura			
GetModelManifest	Concede permissão para obter informações resumidas de uma determinada definição de manifesto de modelo	Leitura	modelmanifest*		
GetRegisterAccountStatus	Concede permissão para obter o status de registro da conta com a IoT FleetWise	Leitura			
GetSignalCatalog	Concede permissão para obter informações resumidas de um catálogo de sinais específico	Leitura	signalcatalog*		
GetStateTemplate	Concede permissão para obter informações resumidas para um determinado modelo de estado	Leitura	statetemplate*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetVehicle	Concede permissão para obter informações resumidas sobre um veículo	Leitura	vehicle*		
GetVehicleStatus	Concede permissão para obter o status das campanhas em execução em um veículo específico	Leitura	vehicle*		
ImportDecoderManifest	Concede permissão para importar um manifesto de decodificador existente	Gravar	decodermanifest*		
ImportSignalCatalog	Concede permissão para criar um catálogo de sinais importando definições existentes	Gravar	signalcatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListCampaigns	Concede permissão para listar campanhas	Leitura			
ListDecoderManifestNetworkInterfaces	Concede permissão para listar interfaces de rede associadas ao manifesto do decodificador existente	Lista	decodermanifest*		
ListDecoderManifestSignals	Concede permissão para listar sinais de manifesto do decodificador	Lista	decodermanifest*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDecoderManifests	Concede permissão para listar todos os manifestos do decodificador, com um filtro opcional no manifesto do modelo	Leitura			
ListFleets	Concede permissão para listar todas as frotas	Leitura			
ListFleetsForVehicle	Concede permissão para listar todas as frotas às quais o veículo fornecido está associado	Leitura	vehicle*		
ListModelManifestNodes	Concede permissão para listar todos os nós para o manifesto de modelo determinado	Lista	modelmanifest*		
ListModelManifests	Concede permissão para listar todos os manifestos do modelo, com um filtro opcional no catálogo de sinais	Leitura			
ListSignalCatalogNodes	Concede permissão para listar todos os nós de determinado catálogo de sinais	Leitura	signalcatalog*		
ListSignalCatalogs	Concede permissão para listar todos os catálogos de sinal	Leitura			
ListStateTemplates	Concede permissão para listar modelos de estado	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	campaign		
			decodermanifest		
			fleet		
			modelmanifest		
			signalcatalog		
			statetemplate		
			vehicle		
ListVehicles	Concede permissão para listar todos os veículos, com um filtro opcional no manifesto do modelo	Leitura			
ListVehiclesInFleet	Concede permissão para listar veículos em uma determinada frota	Leitura	fleet*		
PutEncryptionConfiguration	Concede permissão para ativar ou desativar a criptografia baseada em KMS para o Conta da AWS	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutLoggingOptions	Concede permissão para colocar as opções de registro para o Conta da AWS	Gravar			
RegisterAccount	Concede permissão para registrar e usar Conta da AWS a IoT FleetWise	Gravar			iam:PassRole
TagResource	Concede permissão para adicionar tags a um recurso	Marcação	campaign		
			decodermanifest		
			fleet		
			modelmanifest		
			signalcatalog		
			statetemplate		
			vehicle		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource		Tags	campaign		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	Concede permissão para remover etiquetas de um recurso		decodermanifest		
			fleet		
			modelmanifest		
			signalcatalog		
			statetemplate		
			vehicle		
				aws:TagKeys	
UpdateCampaign	Concede permissão para atualizar a campanha determinada	Gravar	campaign*		
UpdateDecoderManifest	Concede permissão para atualizar uma definição do manifesto de decodificador	Gravar	decodermanifest*		
UpdateFleet	Concede permissão para atualizar a frota	Gravar	fleet*		
UpdateModelManifest	Concede permissão para atualizar a definição de manifesto de modelo fornecida	Gravar	modelmanifest*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateSignalCatalog	Concede permissão para atualizar uma definição de catálogo de sinais específica	Gravar	signalcatalog*		
UpdateStateTemplate	Concede permissão para atualizar o modelo de estado fornecido	Gravar	statetemplate*		
UpdateVehicle	Concede permissão para atualizar o veículo	Gravar	vehicle*		
			decodermanifest		
			modelmanifest		
				iotfleetwise:UpdateToModelManifestArn iotfleetwise:UpdateToDecoderManifestArn	

Tipos de recursos definidos pela AWS IoT FleetWise

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso

também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição para AWS IoT FleetWise

AWS A IoT FleetWise define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais

as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString
iotfleetwise:DestinationArn	Filtra o acesso por ARN de destino da campanha, por exemplo. um ARN de bucket do S3 ou um ARN de fluxo de tempo	ARN
iotfleetwise:Signals	Filtra o acesso por nomes de sinais totalmente qualificados	ArrayOfString
iotfleetwise:UpdateToDecoderManifestArn	Filtra o acesso por uma lista do IoT Decoder Manifest FleetWise ARNs	ARN
iotfleetwise:UpdateToModelManifestArn	Filtra o acesso por uma lista do IoT Model Manifest FleetWise ARNs	ARN

Ações, recursos e chaves de condição do AWS IoT Greengrass

AWS O IoT Greengrass (prefixo do serviço:`greengrass`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS IoT Greengrass
- Tipos de recursos definidos pelo AWS IoT Greengrass
- Chaves de condição do AWS IoT Greengrass

Ações definidas pelo AWS IoT Greengrass

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateRoleToGroup	Concede permissão para associar uma função a um grupo. As permissões da função devem permitir que as principais funções e conectores do Lambda do Greengrass executem ações em outros serviços. AWS	Gravar	group*		
AssociateServiceRoleToAccount	Concede permissão para associar uma função à sua conta. AWS O IoT Greengrass usa essa função para acessar	Gerenciamento de permissões			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	suas funções e recursos de IoT do Lambda. AWS				
CreateConnectorDefinition	Concede permissão para criar uma definição de conector	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnectorDefinitionVersion	Concede permissão para criar uma versão de uma definição de conector existente	Write	connectorDefinition*		
CreateCoreDefinition	Concede permissão para criar uma definição de núcleo	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCoreDefinitionVersion	Concede permissão para criar uma versão de uma definição de núcleo existente. Os grupos do Greengrass devem conter exatamente um núcleo do Greengrass.	Write	coreDefinition*		
CreateDeployment	Concede permissão para criar uma implantação	Write	group*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDeviceDefinition	Concede permissão para criar uma definição de dispositivo	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeviceDefinitionVersion	Concede permissão para criar uma versão de uma definição de dispositivo existente	Write	deviceDefinition*		
CreateFunctionDefinition	Concede permissão para criar uma definição da função do Lambda a ser usada em um grupo que contém uma lista de funções do Lambda e suas configurações	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFunctionDefinitionVersion	Concede permissão para criar uma versão de uma definição de função do Lambda existente	Gravar	functionDefinition*		
CreateGroup	Concede permissão para criar um grupo	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateGroupCertificateAuthority	Concede permissão para criar uma CA para o grupo ou alternar a CA existente	Write	group*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateGroupVersion	Concede permissão para criar uma versão de um grupo que já foi definido	Write	group*		
CreateLoggerDefinition	Concede permissão para criar uma definição do registrador	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLoggerDefinitionVersion	Concede permissão para criar uma versão de uma definição do registrador existente.	Write	loggerDefinition*		
CreateResourceDefinition	Concede permissão para criar uma definição de recurso que contém uma lista de recursos a serem usados em um grupo	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateResourceDefinitionVersion	Concede permissão para criar uma versão de uma definição de recurso existente	Gravar	resourceDefinition*		
CreateSoftwareUpdateJob	Concede permissão para criar um trabalho de AWS IoT que acionará seus núcleos do Greengrass para atualizar o software que estão executando	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSubscriptionDefinition	Concede permissão para criar uma definição de assinatura	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscriptionDefinitionVersion	Concede permissão para criar uma versão de uma definição de assinatura existente	Write	subscriptionDefinition*		
DeleteConnectorDefinition	Concede permissão para excluir uma definição de conector	Write	connectorDefinition*		
DeleteCoreDefinition	Concede permissão para excluir uma definição de núcleo. A exclusão de uma definição que estiver atualmente em uso em uma implantação afeta as implantações futuras	Write	coreDefinition*		
DeleteDeviceDefinition	Concede permissão para excluir uma definição de dispositivo. A exclusão de uma definição que estiver atualmente em uso em uma implantação afeta as implantações futuras	Write	deviceDefinition*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteFunctionDefinition	Concede permissão para excluir a definição de uma função Lambda. A exclusão de uma definição que estiver atualmente em uso em uma implantação afeta as implantações futuras	Write	functionDefinition*		
DeleteGroup	Concede permissão para excluir um grupo que não estiver atualmente em uso em uma implantação	Write	group*		
DeleteLoggerDefinition	Concede permissão para excluir uma definição de registrador. A exclusão de uma definição que estiver atualmente em uso em uma implantação afeta as implantações futuras	Write	loggerDefinition*		
DeleteResourceDefinition	Concede permissão para excluir uma definição de recurso	Write	resourceDefinition*		
DeleteSubscriptionDefinition	Concede permissão para excluir uma definição de assinatura. A exclusão de uma definição que estiver atualmente em uso em uma implantação afeta as implantações futuras	Write	subscriptionDefinition*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateRoleFromGroup	Concede permissão para desassociar a função de um grupo	Write	group*		
DisassociateServiceRoleFromAccount	Concede permissão para desassociar a função de serviço de uma conta. Sem uma função de serviço, as implantações não funcionarão	Write			
Discover	Concede permissão para recuperar as informações necessárias para conectar-se a um núcleo do Greengrass	Read	thing*		
GetAssociatedRole	Concede permissão para recuperar a função associada a um grupo	Read	group*		
GetBulkDeploymentStatus	Concede permissão para retornar o status de uma implantação em massa	Read	bulkDeployment*		
GetConnectivityInfo	Concede permissão para recuperar as informações de conectividade de um núcleo	Read	connectivityInfo*		
GetConnectorDefinition	Concede permissão para recuperar informações sobre uma definição de conector	Read	connectorDefinition*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetConnectorDefinitionVersion	Concede permissão para recuperar informações sobre uma versão de uma definição de conector	Read	connectorDefinition*		
			connectorDefinitionVersion*		
GetCoreDefinition	Concede permissão para recuperar informações sobre uma definição de núcleo	Read	coreDefinition*		
GetCoreDefinitionVersion	Concede permissão para recuperar informações sobre uma versão de definição de núcleo	Read	coreDefinition*		
			coreDefinitionVersion*		
GetDeploymentStatus	Concede permissão para retornar o status de uma implantação	Read	deployment*		
			group*		
GetDeviceDefinition	Concede permissão para recuperar informações sobre a definição de um dispositivo	Read	deviceDefinition*		
GetDeviceDefinitionVersion	Concede permissão para recuperar informações sobre a versão de definição de um dispositivo.	Read	deviceDefinition*		
			deviceDefinitionVersion*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetFunctionDefinition	Concede permissão para recuperar informações sobre uma definição de função do Lambda, como a hora de criação e a versão mais recente	Read	functionDefinition*		
GetFunctionDefinitionVersion	Concede permissão para recuperar informações sobre uma versão de definição de função do Lambda, como quais funções Lambda estão incluídas na versão e suas configurações	Read	functionDefinition*		
			functionDefinitionVersion*		
GetGroup	Concede permissão para recuperar informações sobre um grupo	Read	group*		
GetGroupCertificateAuthority	Concede permissão para retornar a chave pública da CA associada a um grupo	Read	certificateAuthority*		
			group*		
GetGroupCertificateConfiguration	Concede permissão para recuperar a configuração atual da CA usada por um grupo	Read	group*		
GetGroupVersion	Concede permissão para recuperar informações sobre a versão de um grupo	Read	group*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			groupVersion*		
GetLoggerDefinition	Concede permissão para recuperar informações sobre uma definição do registrador	Read	loggerDefinition*		
GetLoggerDefinitionVersion	Concede permissão para recuperar informações sobre uma versão de definição do registrador	Read	loggerDefinition*		
			loggerDefinitionVersion*		
GetResourceDefinition	Concede permissão para recuperar informações sobre uma definição de recurso, como a hora de criação e a versão mais recente	Read	resourceDefinition*		
GetResourceDefinitionVersion	Concede permissão para recuperar informações sobre uma versão de definição do recurso, como quais recursos estão incluídos na versão	Read	resourceDefinition*		
			resourceDefinitionVersion*		
GetServiceRoleForAccount	Concede permissão para recuperar a função de serviço que está anexada a uma conta	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSubscriptionDefinition	Concede permissão para recuperar informações sobre uma definição de assinatura	Read	subscriptionDefinition*		
GetSubscriptionDefinitionVersion	Concede permissão para recuperar informações sobre uma versão de definição de assinatura	Read	subscriptionDefinition*		
			subscriptionDefinitionVersion*		
GetThingRuntimeConfiguration	Concede permissão para recuperar a configuração de runtime de alguma coisa	Read	thingRuntimeConfig*		
ListBulkDeploymentDetailedReports	Concede permissão para recuperar uma lista paginada das implantações que foram iniciadas em uma operação de implantação em massa e seu status de implantação	Read	bulkDeployment*		
ListBulkDeployments	Concede permissão para recuperar uma lista de implantações em massa	List			
ListConnectorDefinitionVersions	Concede permissão para listar as versões da definição de um conector	List	connectorDefinition*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListConnectorDefinitions	Concede permissão para recuperar uma lista de definições do conector	List			
ListCoreDefinitionVersions	Concede permissão para listar as versões de uma definição de núcleo	List	coreDefinition*		
ListCoreDefinitions	Concede permissão para recuperar uma lista de definições de núcleo	List			
ListDeployments	Concede permissão para recuperar uma lista de todas as implantações de um grupo	List	group*		
ListDeviceDefinitionVersions	Concede permissão para listar as versões de uma definição de dispositivo	List	deviceDefinition*		
ListDeviceDefinitions	Concede permissão para recuperar uma lista de definições de dispositivo	List			
ListFunctionDefinitionVersions	Concede permissão para listar as versões da definição de uma função do Lambda	List	functionDefinition*		
ListFunctionDefinitions	Concede permissão para recuperar uma lista de definições da função do Lambda	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListGroupCertificateAuthorities	Concede permissão para recuperar uma lista de atuais CAs para um grupo	Lista	group*		
ListGroupVersions	Concede permissão para listar as versões de um grupo	List	group*		
ListGroups	Concede permissão para recuperar uma lista de grupos	List			
ListLoggerDefinitionVersions	Concede permissão para listar as versões da definição de um registrador	List	loggerDefinition*		
ListLoggerDefinitions	Concede permissão para recuperar uma lista de definições de registrador	List			
ListResourceDefinitionVersions	Concede permissão para listar as versões de uma definição de recurso	List	resourceDefinition*		
ListResourceDefinitions	Concede permissão para recuperar uma lista de definições de recursos	List			
ListSubscriptionDefinitionVersions	Concede permissão para listar as versões da definição de uma assinatura	List	subscriptionDefinition*		
ListSubscriptionDefinitions	Concede permissão para recuperar uma lista de definições de assinatura	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Read	bulkDeployment		
			connectorDefinition		
			coreDefinition		
			deviceDefinition		
			functionDefinition		
			group		
			loggerDefinition		
			resourceDefinition		
			subscriptionDefinition		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ResetDeployments	Concede permissão para redefinir as implantações de um grupo	Write	group*		
StartBulkDeployment	Concede permissão para implantar vários grupos em uma única operação	Write		aws:RequestTag/${TagKey} aws:TagKeys	
StopBulkDeployment	Concede permissão para interromper a execução de uma implantação em massa	Write	bulkDeployment*		
TagResource	Concede permissão para adicionar tags a um recurso	Marcação	bulkDeployment		
			connectorDefinition		
			coreDefinition		
			deviceDefinition		
			functionDefinition		
			group		
			loggerDefinition		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			resourceDefinition		
			subscriptionDefinition		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover etiquetas de um recurso	Marcação	bulkDeployment		
			connectorDefinition		
			coreDefinition		
			deviceDefinition		
			functionDefinition		
			group		
			loggerDefinition		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			resourceDefinition		
			subscriptionDefinition		
				aws:TagKeys	
UpdateConnectivityInfo	Concede permissão para atualizar as informações de conectividade de um núcleo do Greengrass. Todos os dispositivos pertencentes ao grupo que têm esse núcleo receberão essas informações para localizar o núcleo e conectar-se a ele	Write	connectivityInfo*		
UpdateConnectorDefinition	Concede permissão para atualizar a definição de um conector	Write	connectorDefinition*		
UpdateCoreDefinition	Concede permissão para atualizar a definição de um núcleo	Write	coreDefinition*		
UpdateDeviceDefinition	Concede permissão para atualizar a definição de um dispositivo	Write	deviceDefinition*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateFunctionDefinition	Concede permissão para atualizar a definição de uma função do Lambda	Write	functionDefinition*		
UpdateGroup	Concede permissão para atualizar um grupo	Write	group*		
UpdateGroupCertificateConfiguration	Concede permissão para atualizar a hora de expiração do certificado de um grupo	Write	group*		
UpdateLoggerDefinition	Concede permissão para atualizar a definição de um registrador	Write	loggerDefinition*		
UpdateResourceDefinition	Concede permissão para atualizar a definição de um recurso	Write	resourceDefinition*		
UpdateSubscriptionDefinition	Concede permissão para atualizar a definição de uma assinatura	Write	subscriptionDefinition*		
UpdateThingRuntimeConfiguration	Concede permissão para atualizar a configuração de runtime de uma coisa	Write	thingRuntimeConfig*		

Tipos de recursos definidos pelo AWS IoT Greengrass

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso

também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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/	

Tipos de recursos	ARN	Chaves de condição
	cores/${CoreDefinitionId}/versions/${VersionId}	
deviceDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/devices/${DeviceDefinitionId}	aws:ResourceTag/${TagKey}
deviceDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/devices/${DeviceDefinitionId}/versions/${VersionId}	
functionDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/functions/${FunctionDefinitionId}	aws:ResourceTag/${TagKey}
functionDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/functions/${FunctionDefinitionId}/versions/${VersionId}	
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 recursos	ARN	Chaves de condição
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	

Chaves de condição do AWS IoT Greengrass

AWS O IoT Greengrass define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais

as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelo conjunto de valores permitido para cada uma das tags obrigatórias	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelo valor de etiqueta associado ao recurso	String
aws:TagKeys	Filtra o acesso pela presença de etiquetas obrigatórias na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS IoT Greengrass V2

AWS O IoT Greengrass V2 (prefixo do serviço:`greengrass`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS IoT Greengrass V2
- Tipos de recursos definidos pelo AWS IoT Greengrass V2
- Chaves de condição do AWS IoT Greengrass V2

Ações definidas pelo AWS IoT Greengrass V2

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateServiceRoleToAccount	Concede permissão para associar uma função à sua conta. AWS O IoT Greengrass usa essa função para acessar suas funções e recursos de IoT do Lambda. AWS	Gerenciamento de permissões			iam:PassRole
BatchAssociateClientDeviceWithCoreDevice	Concede permissão para associar uma lista de dispositivos clientes a um dispositivo principal	Gravar	coreDevice*		
BatchDisassociateClientDeviceFromCoreDevice	Concede permissão para desassociar uma lista de dispositivos clientes de um dispositivo principal	Gravar	coreDevice*		
CancelDeployment	Concede permissão para cancelar uma implantação	Write	deployment*		iot:CancelJob iot:DeleteThingShadow iot:DescribeJob iot:DescribeThing

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					iot:DescribeThingGroup iot:GetThingShadow iot:UpdateJob iot:UpdateThingShadow
CreateComponentVersion	Concede permissão para criar um componente	Write	component * aws:RequestTag/${TagKey} aws:TagKeys		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDeployment	Concede permissão para criar uma implantação	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 permissão para excluir um componente	Gravar	componentVersion*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteCoreDevice	Concede permissão para excluir um dispositivo principal AWS do IoT Greengrass, que é uma coisa da IoT. AWS Esta operação remove o dispositivo principal da lista de dispositivos principais. Esta operação não exclui a coisa de AWS IoT	Gravar	coreDevice*		iot:DescribeJobExecution
DeleteDeployment	Concede permissão para excluir uma implantação. Para excluir uma implantação ativa, primeiro ela precisa ser cancelada	Gravar	deployment*		iot:DeleteJob
DescribeComponent	Concede permissão para recuperar metadados para uma versão de um componente	Leitura	componentVersion*		
DisassociateServiceRoleFromAccount	Concede permissão para desassociar a função de serviço de uma conta. Sem uma função de serviço, as implantações não funcionarão	Gravar			
GetComponent	Concede permissão para obter a receita de uma versão de um componente	Read	componentVersion*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetComponentVersionArtifact	Concede permissão para obter a URL pré-assinada para fazer download de um artefato de componente público	Leitura	componentVersion*		
GetConnectivityInfo	Concede permissão para recuperar as informações de conectividade de um dispositivo de núcleo do Greengrass	Leitura	connectivityInfo*		iot:GetThingShadow
GetCoreDevice	Concede permissão para recuperar metadados para um dispositivo principal do IoT Greengrass AWS	Leitura	coreDevice*		
GetDeployment	Concede permissão para obter uma implantação	Leitura	deployment*		iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow
GetServiceRoleForAccount	Concede permissão para recuperar a função de serviço que está anexada a uma conta	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListClientDevicesAssociatedWithCoreDevice	Concede permissão para recuperar uma lista paginada de dispositivos cliente associados a um dispositivo principal do AWS IoT Greengrass	Lista	coreDevice*		
ListComponentVersions	Concede permissão para recuperar uma lista paginada de todas as versões de um componente	List	component*		
ListComponents	Concede permissão para recuperar uma lista paginada de resumos de componentes	Lista			
ListCoreDevices	Concede permissão para recuperar uma lista paginada dos principais dispositivos do AWS IoT Greengrass	Lista			
ListDeployments	Concede permissão para recuperar uma lista paginada de implantações	Lista			iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListEffectiveDeployments	Concede permissão para recuperar uma lista paginada de trabalhos de implantação que o IoT Greengrass envia AWS para os dispositivos principais do AWS IoT Greengrass	Lista	coreDevice*		iot:DescribeJob iot:DescribeJobExecution iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow
ListInstalledComponents	Concede permissão para recuperar uma lista paginada dos componentes que um dispositivo principal do AWS IoT Greengrass executa	Lista	coreDevice*		
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	component		
			componentVersion		
			coreDevice		
			deployment		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
ResolveComponentCandidates	Concede permissão para listar componentes que atendem aos requisitos de componente, versão e plataforma de uma implantação	List	componentVersion*		
TagResource	Concede permissão para adicionar tags da a um recurso	Marcação	component		
			componentVersion		
			coreDevice		
			deployment		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover etiquetas de um recurso	Marcação	component		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			componentVersion		
			coreDevice		
			deployment		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateConnectivityInfo	Concede permissão para atualizar as informações de conectividade de um núcleo do Greengrass. Todos os dispositivos pertencentes ao grupo que têm esse núcleo receberão essas informaçõ es para localizar o núcleo e conectar-se a ele	Gravar	connectivityInfo*		iot:GetThingShadow iot:UpdateThingShadow

Tipos de recursos definidos pelo AWS IoT Greengrass V2

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves

são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
connectivityInfo	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/things/${ThingName}/connectivityInfo`	
component	`arn:${Partition}:greengrass:${Region}:${Account}:components:${ComponentName}`	aws:ResourceTag/${TagKey}
componentVersion	`arn:${Partition}:greengrass:${Region}:${Account}:components:${ComponentName}:versions:${ComponentVersion}`	aws:ResourceTag/${TagKey}
coreDevice	`arn:${Partition}:greengrass:${Region}:${Account}:coreDevices:${CoreDeviceThingName}`	aws:ResourceTag/${TagKey}
deployment	`arn:${Partition}:greengrass:${Region}:${Account}:deployments:${DeploymentId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS IoT Greengrass V2

AWS O IoT Greengrass V2 define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso verificando key/value os pares de tags incluídos na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso verificando key/value os pares de tags associados a um recurso específico	String
aws:TagKeys	Filtra o acesso verificando as chaves de etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para trabalhos de AWS IoT DataPlane

AWS O IoT Jobs DataPlane (prefixo do serviço:`iotjobsdata`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS IoT Jobs DataPlane
- Tipos de recursos definidos por AWS IoT Jobs DataPlane
- Chaves de condição para trabalhos AWS de IoT DataPlane

Ações definidas pelo AWS IoT Jobs DataPlane

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando

usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeJobExecution	Concede permissão para descrever a execução de um trabalho	Leitura	thing*		
				iot:JobId	
GetPendingJobExecutions	Concede permissão para obter a lista de todos os trabalhos de uma coisa que não estão em um estado terminal	Leitura	thing*		
StartNextPendingJobExecution	Concede permissão para obter e iniciar a próxima execução de trabalho pendente de uma coisa	Gravar	thing*		
UpdateJobExecution	Concede permissão para atualizar a execução de um trabalho	Gravar	thing*		
				iot:JobId	

Tipos de recursos definidos por AWS IoT Jobs DataPlane

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
thing	`arn:${Partition}:iot:${Region}:${Account}:thing/${ThingName}`	

Chaves de condição para trabalhos AWS de IoT DataPlane

AWS O IoT Jobs DataPlane define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
iot:JobId	Filtra o acesso por jobID para iotjobsdata: e iotjobsdata: DescribeJobExecution UpdateJobExecution APIs	String

Ações, recursos e chaves de condição para integrações gerenciadas de AWS IoT

AWS As integrações gerenciadas de IoT (prefixo do serviço:`iotmanagedintegrations`) fornecem os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelas integrações gerenciadas AWS de IoT
- Tipos de recursos definidos pelas integrações AWS gerenciadas de IoT
- Chaves de condição para AWS integrações gerenciadas de IoT

Ações definidas pelas integrações gerenciadas AWS de IoT

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de

recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAccountAssociation	Concede permissão para criar uma nova associação de conta	Gravar		aws:RequestTag/${TagKey} aws:TagKeys iotmanagedintegrations:connectorDestinationId	
CreateCloudConnector	Concede permissão para criar um novo conector de nuvem	Gravar			
CreateConnectorDestination	Concede permissão para criar um novo destino de conector	Gravar		iotmanagedintegrations:cloudConnectorId	
CreateCredentialLocker	Concede permissão para criar um armário de credenciais de produto	Gravar		aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
CreateDestination	Concede permissão para criar um novo destino	Gravar			
CreateEventLogConfiguration	Concede permissão para criar uma nova configuração de evento	Gravar			
CreateManagedThing	Concede permissão para criar uma nova coisa gerenciada	Gravar	credential-locker		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNotificationConfiguration	Concede permissão para criar uma nova configuração de notificação	Gravar			
CreateOtaTask	Concede permissão para criar uma nova tarefa ota	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOtaTaskConfiguration	Concede permissão para criar uma nova configuração de tarefa ota	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateProvisioningProfile	Concede permissão para criar um novo perfil de aprovisionamento	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccountAssociation	Concede permissão para excluir uma associação de conta	Gravar	account-association*		
DeleteCloudConnector	Concede permissão para excluir um conector de nuvem	Gravar		iotmanagedintegrations:cloudConnectorId	
DeleteConnectorDestination	Concede permissão para excluir um destino de conector	Gravar			
DeleteCredentialLocker	Concede permissão para excluir um armário de credenciais	Gravar	credential-locker*		
DeleteDestination	Concede permissão para excluir o destino	Gravar			
DeleteEventLogConfiguration	Concede permissão para excluir a configuração do registro de eventos	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteManagedThing	Concede permissão para excluir algo gerenciado	Gravar	managed-thing*		
DeleteNotificationConfiguration	Concede permissão para excluir a configuração de notificação	Gravar			
DeleteOtaTask	Concede permissão para excluir uma tarefa ota	Gravar	ota-task*		
DeleteOtaTaskConfiguration	Concede permissão para excluir a configuração da tarefa ota	Gravar			
DeleteProvisioningProfile	Concede permissão para excluir o perfil de aprovisionamento	Gravar	provisioning-profile*		
DeregisterAccountAssociation	Concede permissão para cancelar o registro da associação de contas	Gravar	account-association*		
			managed-thing*		
GetAccountAssociation	Concede permissão para obter informações sobre uma associação de conta	Leitura	account-association*		
GetCloudConnector	Concede permissão para obter informações sobre um conector de nuvem	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetConnectorDestination	Concede permissão para obter informações sobre um destino na nuvem	Leitura			
GetCredentialLocker	Concede permissão para obter informações sobre um armário de credenciais	Leitura	credential-locker*		
GetCustomEndpoint	Concede permissão para obter informações sobre um endpoint personalizado	Leitura			
GetDefaultEncryptionConfiguration	Concede permissão para obter informações sobre uma configuração de criptografia padrão	Leitura			
GetDestination	Concede permissão para obter informações sobre um destino	Leitura			
GetDeviceDiscovery	Concede permissão para obter informações sobre a descoberta de um dispositivo	Leitura			
GetEventLogConfiguration	Concede permissão para obter informações sobre uma configuração de registro de eventos	Leitura			
GetHubConfiguration	Concede permissão para obter informações sobre a configuração de um hub	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetManagedThing	Concede permissão para obter informações sobre algo gerenciado	Leitura	managed-thing*		
GetManagedThingCapabilities	Concede permissão para obter o relatório de capacidade de uma coisa gerenciada	Leitura	managed-thing*		
GetManagedThingConnectivityData	Concede permissão para obter os dados de conectividade de uma coisa gerenciada	Leitura	managed-thing*		
GetManagedThingMetaData	Concede permissão para obter as informações de metadados de uma coisa gerenciada	Leitura	managed-thing*		
GetManagedThingState	Concede permissão para obter as informações de estado do dispositivo para uma coisa gerenciada	Leitura	managed-thing*		
GetNotificationConfiguration	Concede permissão para obter informações para uma configuração de notificação	Leitura			
GetOtaTask	Concede permissão para obter informações para uma tarefa ota	Leitura	ota-task*		
GetOtaTaskConfiguration	Concede permissão para obter informações para uma configuração de tarefa ota	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetProvisioningProfile	Concede permissão para obter informações para um perfil de aprovisionamento	Leitura	provisioning-profile*		
GetRuntimeLogConfiguration	Concede permissão para obter informações para uma configuração de log de tempo de execução	Leitura			
GetSchemaVersion	Concede permissão para obter informações para uma versão de um esquema	Leitura			
ListAccountAssociations	Concede permissão para listar informações para associações de contas	Lista			
ListCloudConnectors	Concede permissão para listar informações para conectores de nuvem	Lista			
ListConnectorDestinations	Concede permissão para listar informações para destinos de conectores	Lista			
ListCredentialLockers	Concede permissão para listar informações para armários de credenciais	Lista			
ListDestinations	Concede permissão para listar informações para destinos	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDeviceDiscoveries	Concede permissão para listar informações para descobertas de dispositivos	Lista			
ListDiscoveredDevices	Concede permissão para listar informações do dispositivo descoberto em uma descoberta de dispositivo	Leitura			
ListEventLogConfigurations	Concede permissão para listar informações para configurações de registro de eventos	Leitura			
ListManagedThingAccountAssociations	Concede permissão para listar informações para associações entre itens gerenciados e associações de contas	Lista			
ListManagedThingSchemas	Concede permissão para listar esquemas associados a uma coisa gerenciada	Leitura	managed-thing*		
ListManagedThings	Concede permissão para listar informações de itens gerenciados	Lista			
ListNotificationConfigurations	Concede permissão para listar informações para configurações de notificação	Leitura			
ListOtaTaskConfigurations	Concede permissão para listar informações para configurações de tarefas ota	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListOtaTaskExecutions	Concede permissão para listar informações para execuções de tarefas ota	Leitura	ota-task*		
ListOtaTasks	Concede permissão para listar informações para tarefas ota	Lista			
ListProvisioningProfiles	Concede permissão para listar informações para perfis de aprovisionamento	Lista			
ListSchemaVersions	Concede permissão para listar informações para esquemas	Lista			
ListTagsForResource	Concede permissão para listar etiquetas para o recurso especificado	Leitura	account-association		
			credential-locker		
			managed-thing		
			ota-task		
			provisioning-profile		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutDefaultEncryptionConfiguration	Concede permissão para atualizar as configurações padrão de uma configuração de criptografia	Gravar			
PutHubConfiguration	Concede permissão para atualizar a configuração de um hub	Gravar			
PutRuntimeLogConfiguration	Concede permissão para atualizar uma configuração de log de tempo de execução	Gravar			
RegisterAccountAssociation	Concede permissão para registrar uma associação de conta a uma coisa gerenciada	Gravar	account-association*		
			managed-thing*		
RegisterCustomEndpoint	Concede permissão para registrar um endpoint personalizado	Gravar			
ResetRuntimeLogConfiguration	Concede permissão para redefinir uma configuração de registro de tempo de execução	Gravar			
SendConnectorEvent	Concede permissão para enviar um evento de conector	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SendManagedThingCommand	Concede permissão para enviar um comando para uma coisa gerenciada	Gravar	managed-thing*		
			account-association		
StartAccountAssociationRefresh	Concede permissão para iniciar uma atualização dos tokens de acesso associados a uma associação de conta	Gravar	account-association*		
StartDeviceDiscovery	Concede permissão para iniciar a descoberta de um dispositivo	Gravar	account-association		
			managed-thing		
TagResource	Concede permissão para adicionar tags para o recurso especificado	Tags	account-association		
			credential-locker		
			managed-thing		
			ota-task		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			provisioning-profile		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover tags do recurso especificado	Tags	account-association		
			credential-locker		
			managed-thing		
			ota-task		
			provisioning-profile		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateAccountAssociation	Concede permissão para atualizar uma associação de conta	Gravar	account-association*		
UpdateCloudConnector	Concede permissão para atualizar um conector de nuvem	Gravar		iotmanagedintegrations:cloudConnectorId	
UpdateConnectorDestination	Concede permissão para atualizar o destino de um conector	Gravar			
UpdateDestination	Concede permissão para atualizar um destino	Gravar			
UpdateEventLogConfiguration	Concede permissão para atualizar uma configuração de registro de eventos	Gravar			
UpdateManagedThing	Concede permissão para atualizar uma coisa gerenciada	Gravar	managed-thing* credential-locker		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateNotification Configuration	Concede permissão para atualizar uma configuração de notificação	Gravar			
UpdateOtaTask	Concede permissão para atualizar uma tarefa ota	Gravar	ota-task*		

Tipos de recursos definidos pelas integrações AWS gerenciadas de IoT

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição para AWS integrações gerenciadas de IoT

AWS As integrações gerenciadas de IoT definem as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por um par de chave valor da etiqueta que é permitido na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso por um par de chave e valor da etiqueta de um recurso.	String
aws:TagKeys	Filtra o acesso pelas chaves de etiqueta que são transmitidas na solicitação	ArrayOfString
iotmanagedintegrat	Filtra o acesso pelo CloudConnectorId	String

Chaves de condição	Descrição	Tipo
ions:clou dConnectorId		
iotmanage dintegrat ions:conn ectorDest inationId	Filtra o acesso pelo ConnectorDestinationId	String

Ações, recursos e chaves de condição para AWS IoT SiteWise

AWS A IoT SiteWise (prefixo do serviço:`iotsitewise`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela AWS IoT SiteWise
- Tipos de recursos definidos pela AWS IoT SiteWise
- Chaves de condição para AWS IoT SiteWise

Ações definidas pela AWS IoT SiteWise

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateAssets	Concede permissão para associar um ativo filho a um ativo pai por uma hierarquia	Gravar	asset*		
AssociateTimeSeriesToAssetProperty	Concede permissão para associar uma série temporal a uma propriedade de ativo	Gravar	asset*		
			time-series*		
BatchAssociateProjectAssets	Concede permissão para associar ativos a um projeto	Write	project*		
BatchDisassociateProjectAssets	Concede permissão para desassociar ativos de um projeto	Gravar	project*		
BatchGetAssetPropertyAggregates	Concede permissão para recuperar agregados computados para várias propriedades do ativo	Leitura	asset		
			time-series		
BatchGetAssetPropertyValue	Concede permissão para recuperar o valor mais recente de várias propriedades do ativo	Leitura	asset		
			time-series		
BatchGetAssetPropertyValueHistory	Concede permissão para recuperar o histórico do valor de várias propriedades do ativo	Leitura	asset		
			time-series		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchPutAssetPropertyValue	Concede permissão para colocar valores de propriedade para propriedades de ativos	Write	asset		
			time-series		
CreateAccessPolicy	Concede permissão para criar uma política de acesso para um portal ou um projeto	Write	portal		
			project		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAsset	Concede permissão para criar um ativo usando um modelo de ativo	Write	asset-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssetModel	Concede permissão para criar um modelo de ativo	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAssetModelCompositeModel	Concede permissão para criar um modelo composto de modelo de ativo dentro de um modelo de ativo	Gravar	asset-model*		
CreateBulkImportJob	Concede permissão para criar um trabalho de importação em massa	Gravar			
CreateComputationModel	Concede permissão para criar um modelo computacional	Gravar	asset		
			asset-model		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDashboard	Concede permissão para criar um painel em um projeto	Gravar	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDataset	Concede permissão para criar um conjunto de dados	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateGateway	Concede permissão para criar um gateway	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePortal	Concede permissão para criar um portal	Write		aws:RequestTag/${TagKey} aws:TagKeys	sso:CreateManagedApplicationInstance sso:DescribeRegisteredRegions
CreateProject	Concede permissão para criar um projeto em um portal	Write	portal*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteAccessPolicy	Concede permissão para excluir uma política de acesso	Write	access-policy*		
DeleteAsset	Concede permissão para excluir um ativo	Write	asset*		
DeleteAssetModel	Concede permissão para excluir um modelo de ativo	Gravar	asset-model*		
DeleteAssetModelCompositeModel	Concede permissão para excluir um modelo composto de modelo de ativo	Gravar	asset-model*		
DeleteAssetModelInterfaceRelationship	Concede permissão para excluir uma relação entre o modelo do ativo e a interface	Gravar	asset-model*		
DeleteComputationModel	Concede permissão para excluir um modelo de computação	Gravar	computation-model*		
DeleteDashboard	Concede permissão para excluir um painel	Gravar	dashboard*		
DeleteDataset	Concede permissão para excluir um conjunto de dados	Gravar	dataset*		
DeleteGateway	Concede permissão para excluir um gateway	Write	gateway*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeletePortal	Concede permissão para excluir um portal	Write	portal*		sso:DeleteManagedApplicationInstance
DeleteProject	Concede permissão para excluir um projeto	Gravar	project*		
DeleteTimeSeries	Concede permissão para excluir uma série temporal	Gravar	asset		
			time-series		
DescribeAccessPolicy	Concede permissão para descrever uma política de acesso	Leitura	access-policy*		
DescribeAction	Concede permissão para descrever ações	Leitura	asset		
			computation-model		
DescribeAsset	Concede permissão para descrever um ativo	Leitura	asset*		
DescribeAssetCompositeModel	Concede permissão para descrever um modelo composto de ativo	Leitura	asset*		
DescribeAssetModel	Concede permissão para descrever um modelo de ativo	Leitura	asset-model*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeAssetModelCompositeModel	Concede permissão para descrever um modelo composto de modelo de ativos	Leitura	asset-model*		
DescribeAssetModelInterfaceRelationship	Concede permissão para descrever uma relação entre o modelo de ativos e a interface	Leitura	asset-model*		
DescribeAssetProperty	Concede permissão para descrever uma propriedade de ativo	Leitura	asset*		
DescribeBulkImportJob	Concede permissão para descrever um trabalho de importação em massa	Leitura			
DescribeComputationModel	Concede permissão para descrever um modelo de computação	Leitura	computation-model*		
DescribeComputationModelExecutionSummary	Concede permissão para descrever o resumo da execução do modelo computacional	Leitura	computation-model*		
			asset		
DescribeDashboard	Concede permissão para descrever um painel	Leitura	dashboard*		
DescribeDataset	Concede permissão para descrever o conjunto de dados	Leitura	dataset*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeDefaultEncryptionConfiguration	Concede permissão para descrever a configuração de criptografia padrão para o Conta da AWS	Leitura			
DescribeExecution	Concede permissão para descrever uma execução	Leitura			
DescribeGateway	Concede permissão para descrever um gateway	Read	gateway*		
DescribeGatewayCapabilityConfiguration	Concede permissão para descrever uma configuração de capacidade para um gateway	Leitura	gateway*		
DescribeLoggingOptions	Concede permissão para descrever as opções de registro para o Conta da AWS	Leitura			
DescribePortal	Concede permissão para descrever um portal	Read	portal*		
DescribeProject	Concede permissão para descrever um projeto	Leitura	project*		
DescribeStorageConfiguration	Concede permissão para descrever a configuração de armazenamento do Conta da AWS	Leitura			
DescribeTimeSeries	Concede permissão para descrever uma série temporal	Leitura	asset		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			time-series		
				aws:RequestTag/${TagKey} aws:TagKeys	
DisassociateAssets	Concede permissão para desassociar um ativo filho de um ativo pai por uma hierarquia	Gravar	asset*		
DisassociateTimeSeriesFromAssetProperty	Concede permissão para desassociar uma série temporal de uma propriedade de ativo	Gravar	asset*		
			time-series*		
EnableSiteWiseIntegration [somente permissão]	Concede permissão para permitir a SiteWise integração da IoT com outros serviços	Gravar			
ExecuteAction	Concede permissão para executar ações	Gravar	asset		
			computation-model		
ExecuteQuery	Concede permissão para executar uma consulta	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAssetPropertyAggregates	Concede permissão para recuperar agregados computados para uma propriedade de ativo	Read	asset		
			time-series		
GetAssetPropertyValue	Concede permissão para recuperar o valor mais recente de uma propriedade de ativo	Read	asset		
			time-series		
GetAssetPropertyValueHistory	Concede permissão para recuperar o histórico de valor de uma propriedade de ativo	Leitura	asset		
			time-series		
GetInterpolatedAssetPropertyValues	Concede permissão para recuperar valores interpolados de uma propriedade de ativo	Leitura	asset		
			time-series		
InvokeAssistant	Concede permissão para invocar um assistente	Leitura			
ListAccessPolicies	Concede permissão para listar todas as políticas de acesso para uma identidade ou um recurso	Lista	portal		
			project		
ListActions	Concede permissão para listar todas as ações	Lista	asset		
			computation-model		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAssetModelCompositeModels	Concede permissão para listar todos os modelos compostos de modelos de ativos	Lista	asset-model*		
ListAssetModelProperties	Concede permissão para listar propriedades dos modelos de ativos	Lista	asset-model*		
ListAssetModels	Concede permissão para listar todos os modelos de ativos	Lista			
ListAssetProperties	Concede permissão para listar propriedades de ativos	Lista	asset*		
ListAssetRelationships	Concede permissão para listar o gráfico de relacionamento de ativo para um ativo	List	asset*		
ListAssets	Concede permissão para listar todos os ativos	Lista	asset-model		
ListAssociatedAssets	Concede permissão para listar todos os ativos associados a um ativo por uma hierarquia	Lista	asset*		
ListBulkImportJobs	Concede permissão para listar trabalhos de importação em massa	Lista			
ListCompositionRelationships	Concede permissão para listar todas as relações de composição de modelos de ativos	Lista	asset-model*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListComputationModelDataBindingUsages	Concede permissão para listar os usos de vinculação de dados do modelo de computação	Lista	asset		
			asset-model		
ListComputationModelResolveToResources	Concede permissão para listar a resolução do modelo de computação aos recursos	Lista	computation-model*		
ListComputationModels	Concede permissão para listar todos os modelos de computação	Lista			
ListDashboards	Concede permissão para listar todos os painéis em um projeto	Lista	project*		
ListDatasets	Concede permissão para listar todos os conjuntos de dados	Lista			
ListExecutions	Concede permissão para listar execuções	Lista	asset		
			computation-model		
ListGateways	Concede permissão para listar todos os gateways	Lista			
ListInterfaceRelationships	Concede permissão para listar todos os modelos de ativos que são aplicados por uma interface	Lista	asset-model*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListPortals	Concede permissão para listar todos os portais	List			
ListProjectAssets	Concede permissão para listar todos os ativos associados a um projeto	List	project*		
ListProjects	Concede permissão para listar todos os projetos em um portal	List	portal*		
ListTagsForResource	Concede permissão para listar todas as etiquetas de um recurso	Leitura	access-policy		
			asset		
			asset-model		
			computation-model		
			dashboard		
			dataset		
			gateway		
			portal		
			project		
			time-series		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
ListTimeSeries	Concede permissão para listar séries temporais	Lista	asset		
PutAssetModelInterfaceRelationship	Concede permissão para criar um relacionamento entre o modelo de ativos e a interface	Gravar	asset-model*		
PutDefaultEncryptionConfiguration	Concede permissão para definir a configuração de criptografia padrão para o Conta da AWS	Gravar			
PutLoggingOptions	Concede permissão para definir opções de registro para o Conta da AWS	Gravar			
PutStorageConfiguration	Concede permissão para definir as configurações de armazenamento para o Conta da AWS	Gravar			
TagResource	Concede permissão para marcar um recurso	Marcação	access-policy		
			asset		
			asset-model		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			computation-model		
			dashboard		
			dataset		
			gateway		
			portal		
			project		
			time-series		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para desmarcar um recurso	Marcação	access-policy		
			asset		
			asset-model		
			computation-model		
			dashboard		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			dataset		
			gateway		
			portal		
			project		
			time-series		
				aws:TagKeys	
UpdateAccessPolicy	Concede permissão para atualizar uma política de acesso	Write	access-policy*		
UpdateAsset	Concede permissão para atualizar um ativo	Write	asset*		
UpdateAssetModel	Concede permissão para atualizar um modelo de ativo	Gravar	asset-model*		
UpdateAssetModelCompositeModel	Concede permissão para atualizar um modelo composto de modelo de ativo	Gravar	asset-model*		
UpdateAssetModelPropertyRouting [somente permissão]	Concede permissão para atualizar o roteamento de uma AssetModel propriedade	Gravar	asset-model*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateAssetProperty	Concede permissão para atualizar uma propriedade de ativo	Gravar	asset*		
UpdateComputationModel	Concede permissão para atualizar um modelo de computação	Gravar	computation-model*		
			asset		
			asset-model		
UpdateDashboard	Concede permissão para atualizar um painel	Gravar	dashboard*		
UpdateDataset	Concede permissão para atualizar um conjunto de dados	Gravar	dataset*		
UpdateGateway	Concede permissão para atualizar um gateway	Write	gateway*		
UpdateGatewayCapabilityConfiguration	Concede permissão para atualizar uma configuração de capacidade para um gateway	Write	gateway*		
UpdatePortal	Concede permissão para atualizar um portal	Write	portal*		
UpdateProject	Concede permissão para atualizar um projeto	Gravar	project*		

Tipos de recursos definidos pela AWS IoT SiteWise

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Tipos de recursos	ARN	Chaves de condição
dataset	`arn:${Partition}:iotsitewise:${Region}:${Account}:dataset/${DatasetId}`	aws:ResourceTag/${TagKey}
computation-model	`arn:${Partition}:iotsitewise:${Region}:${Account}:computation-model/${ComputationModelId}`	aws:ResourceTag/${TagKey}

Chaves de condição para AWS IoT SiteWise

AWS A IoT SiteWise define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso pelos pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas anexadas ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta na solicitação	ArrayOfString
iotsitewise:assetHierarchyPath	Filtra o acesso por um caminho da hierarquia de ativos, que é a sequência de caracteres do ativo IDs na hierarquia do ativo, cada um separado por uma barra	String
iotsitewise:childAssetId	Filtra o acesso pelo ID de um ativo filho que está sendo associado a um ativo pai	String

Chaves de condição	Descrição	Type
iotsitewise:group	Filtra o acesso pelo ID de um grupo de login AWS único	String
iotsitewise:iam	Filtra o acesso pelo ID de uma identidade AWS do IAM	String
iotsitewise:isAssociatedWithAssetProperty	Filtra o acesso por Data Streams (fluxos de dados) associados ou não às propriedades do ativo	String
iotsitewise:portal	Filtra o acesso pelo ID de um portal	String
iotsitewise:project	Filtra o acesso pelo ID de um projeto	String
iotsitewise:propertyAlias	Filtra o acesso pelo alias da propriedade	String
iotsitewise:propertyId	Filtra o acesso pelo ID de uma propriedade de ativo	String
iotsitewise:user	Filtra o acesso pelo ID de um usuário de login AWS único	String

Ações, recursos e chaves de condição para AWS IoT TwinMaker

AWS A IoT TwinMaker (prefixo do serviço:`iottwinmaker`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela AWS IoT TwinMaker
- Tipos de recursos definidos pela AWS IoT TwinMaker
- Chaves de condição para AWS IoT TwinMaker

Ações definidas pela AWS IoT TwinMaker

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de

recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchPutPropertyValues	Concede permissão para definir valores para várias propriedades de séries temporais	Gravar	workspace*		iottwinmaker:GetComponentType iottwinmaker:GetEntity iottwinmaker:GetWorkspace
			entity		
CancelMetadataTransferJob	Concede permissão para cancelar um trabalho de transferência de metadados	Gravar	metadataTransferJob*		
CreateComponentType	Concede permissão para criar um componentType	Gravar	workspace*		
				aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
CreateEntity	Concede permissão para criar um entidade	Gravar	workspace*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMetadataTransferJob	Concede permissão para criar um trabalho de transferência de metadados	Gravar			
CreateScene	Concede permissão para criar uma cena	Gravar	workspace*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSyncJob	Concede permissão para criar um trabalho de sincronização	Gravar	workspace*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspace	Concede permissão para criar um Workspace	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteComponentType	Concede permissão para excluir um componentType	Gravar	componentType* workspace*		
DeleteEntity	Concede permissão para excluir uma entidade	Gravar	entity* workspace*		
DeleteScene	Concede permissão para excluir uma cena	Gravar	scene* workspace*		
DeleteSyncJob	Concede permissão para excluir um trabalho de sincronização	Gravar	syncJob* workspace*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteWorkspace	Concede permissão para excluir um Workspace	Gravar	workspace*		
ExecuteQuery	Concede permissão para executar uma consulta	Leitura	workspace*		
GetComponentType	Concede permissão para obter um componentType	Leitura	componentType*		
			workspace*		
GetEntity	Concede permissão para obter uma entidade	Leitura	entity*		
			workspace*		
GetMetadataTransferJob	Concede permissão para obter um trabalho de transferência de metadados	Leitura	metadataTransferJob*		
GetPricingPlan	Concede permissão para obter um plano de preços	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetPropertyValue	Concede permissão para recuperar os valores da propriedade	Leitura	workspace*		iottwinmaker:GetComponentType iottwinmaker:GetEntity iottwinmaker:GetWorkspace
			componentType		
			entity		
GetPropertyValueHistory	Concede permissão para recuperar o histórico de valor de uma série temporal	Leitura	workspace*		iottwinmaker:GetComponentType iottwinmaker:GetEntity iottwinmaker:GetWorkspace
			componentType		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			entity		
GetScene	Concede permissão para obter uma cena	Leitura	scene*		
			workspace*		
GetSyncJob	Concede permissão para obter um trabalho de sincronização	Leitura	syncJob*		
			workspace*		
GetWorkspace	Concede permissões para obter um workspace	Leitura	workspace*		
ListComponentTypes	Concede permissão para listar todos os componentTypes em um workspace	Lista	workspace*		
ListComponents	Concede permissão para listar componentes anexados a uma entidade	Lista	entity*		
			workspace*		
ListEntities	Concede permissão para listar todas as entidades em um workspace	Lista	workspace*		
ListMetadataTransferJobs	Concede permissão para listar todos os trabalhos de transferência de metadados	Lista			
ListProperties	Concede permissão para listar propriedades de um componente de entidade	Lista	entity*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			workspace*		
ListScenes	Concede permissão para listar todas as cenas em um workspace	Lista	workspace*		
ListSyncJobs	Concede permissão para listar todos os trabalhos de sincronização em um espaço de trabalho	Lista	workspace*		
ListSyncResources	Concede permissão para listar todos os recursos de sincronização de um trabalho de sincronização	Lista	syncJob*		
			workspace*		
ListTagsForResource	Concede permissão para listar todas as etiquetas de um recurso	Lista	componentType		
			entity		
			scene		
			syncJob		
			workspace		
				aws:ResourceTag/${TagKey}	
ListWorkspaces	Concede permissão para listar todos os workspace	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para marcar um recurso	Marcação	componentType		
			entity		
			scene		
			syncJob		
			workspace		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso	Tags	componentType		
			entity		
			scene		
			syncJob		
			workspace		
				aws:TagKeys	
UpdateComponentType	Concede permissão para atualizar um componentType	Gravar	componentType*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			workspace*		
UpdateEntity	Concede permissão para atualizar uma entidade	Gravar	entity*		
			workspace*		
UpdatePricingPlan	Concede permissão para atualizar um plano de preços	Gravar			
UpdateScene	Concede permissão para atualizar uma cena	Gravar	scene*		
			workspace*		
UpdateWorkspace	Concede permissão para criar um workspace	Gravar	workspace*		

Tipos de recursos definidos pela AWS IoT TwinMaker

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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/${TagKey}
scene	arn:${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}	

Chaves de condição para AWS IoT TwinMaker

AWS A IoT TwinMaker define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso pelos pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas anexadas ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta na solicitação	ArrayOfString
iottwinmaker:destinationType	Filtra o acesso por tipo de destino do trabalho de transferência de metadados	ArrayOfString
iottwinmaker:linkedServices	Filtra o acesso por espaço de trabalho vinculado a serviços	ArrayOfString
iottwinmaker:sourceType	Filtra o acesso por tipo de origem do trabalho de transferência de metadados	ArrayOfString

Ações, recursos e chaves de condição do AWS IoT Wireless

AWS O IoT Wireless (prefixo do serviço`iotwireless`:) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS IoT Wireless
- Tipos de recursos definidos pelo AWS IoT Wireless

- Chaves de condição do AWS IoT Wireless

Ações definidas pelo AWS IoT Wireless

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateAwsAccountWithPartnerAccount	Concede permissão para vincular contas de parceiros com Conta da AWS	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
AssociateMulticastGroupWithFuotaTask	Concede permissão para associar o MulticastGroup com FuotaTask	Gravar	FuotaTask*		
			MulticastGroup*		
AssociateWirelessDeviceWithFuotaTask	Concede permissão para associar o dispositivo sem fio a FuotaTask	Gravar	FuotaTask*		
			WirelessDevice*		
AssociateWirelessDeviceWithMulticastGroup	Concede permissão para associar o WirelessDevice com MulticastGroup	Gravar	MulticastGroup*		
			WirelessDevice*		
AssociateWirelessD	Concede permissão para associar o dispositivo sem fio a uma coisa de AWS IoT para	Gravar	WirelessDevice*		iot:DescribeThing

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
eviceWithThing	um determinado wirelessDeviceId		thing*		
AssociateWirelessGatewayWithCertificate	Concede permissão para associar um WirelessGateway ao certificado IoT Core Identity	Gravar	WirelessGateway*		
			cert*		
AssociateWirelessGatewayWithThing	Concede permissão para associar o gateway sem fio a uma coisa de AWS IoT para uma determinada coisa wirelessGatewayId	Gravar	WirelessGateway*		iot:DescribeThing
			thing*		
CancelMulticastGroupSession	Concede permissão para cancelar a MulticastGroup sessão	Gravar	MulticastGroup*		
CreateDestination	Concede permissão para criar um recurso de destino	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeviceProfile	Concede permissão para criar um DeviceProfile recurso	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateFuotaTask	Concede permissão para criar um FuotaTask recurso	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateMulticastGroup	Concede permissão para criar um MulticastGroup recurso	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateNetworkAnalyzerConfiguration	Concede permissão para criar um NetworkAnalyzerConfiguration recurso	Gravar	MulticastGroup*		
			WirelessDevice*		
			WirelessGateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateServiceProfile	Concede permissão para criar um ServiceProfile recurso	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWirelessDevice	Concede permissão para criar um WirelessDevice recurso com determinado destino	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWirelessGateway	Concede permissão para criar um WirelessGateway recurso	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWirelessGatewayTask	Concede permissão para criar uma tarefa para uma determinada WirelessGateway	Gravar	WirelessGateway*		
CreateWirelessGatewayTaskDefinition	Concede permissão para criar uma definição de WirelessGateway tarefa	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDestination	Concede permissão para excluir um destino	Gravar	Destination*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteDeviceProfile	Concede permissão para excluir um DeviceProfile	Gravar	DeviceProfile*		
DeleteFuotaTask	Concede permissão para excluir o FuotaTask	Gravar	FuotaTask*		
DeleteMulticastGroup	Concede permissão para excluir o MulticastGroup	Gravar	MulticastGroup*		
DeleteNetworkAnalyzerConfiguration	Concede permissão para excluir o NetworkAnalyzerConfiguration	Gravar	NetworkAnalyzerConfiguration*		
DeleteQueuedMessages	Concede permissão para excluir QueuedMessages	Gravar			
DeleteServiceProfile	Concede permissão para excluir um ServiceProfile	Gravar	ServiceProfile*		
DeleteWirelessDevice	Concede permissão para excluir um WirelessDevice	Gravar	WirelessDevice*		
DeleteWirelessDeviceImportTask	Concede permissão para excluir a tarefa de importação de dispositivos sem fio	Gravar	ImportTask*		
DeleteWirelessGateway	Concede permissão para excluir um WirelessGateway	Gravar	WirelessGateway*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteWirelessGatewayTask	Concede permissão para excluir a tarefa de uma determinada WirelessGateway	Gravar	WirelessGateway*		
DeleteWirelessGatewayTaskDefinition	Concede permissão para excluir uma definição de WirelessGateway tarefa	Gravar	WirelessGatewayTaskDefinition*		
DeregisterWirelessDevice	Concede permissão para cancelar o registro de um dispositivo sem fio	Gravar	WirelessDevice*		
DisassociateAwsAccountFromPartnerAccount	Concede permissão para desassociar uma Conta da AWS conta de parceiro	Gravar	SidewalkAccount*		
DisassociateMulticastGroupFromFuotaTask	Concede permissão para desassociar o formulário MulticastGroup FuotaTask	Gravar	FuotaTask*		
			MulticastGroup*		
DisassociateWirelessDeviceFromFuotaTask	Concede permissão para desassociar o dispositivo sem fio do FuotaTask	Gravar	FuotaTask*		
			WirelessDevice*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateWirelessDeviceFromMulticastGroup	Concede permissão para desassociar o dispositivo sem fio do MulticastGroup	Gravar	MulticastGroup*		
			WirelessDevice*		
DisassociateWirelessDeviceFromThing	Concede permissão para desassociar um dispositivo sem fio de uma coisa de AWS IoT	Gravar	WirelessDevice*		iot:DescribeThing
			thing*		
DisassociateWirelessGatewayFromCertificate	Concede permissão para desassociar um WirelessGateway de um certificado de identidade principal de IoT	Gravar	WirelessGateway*		
			cert*		
DisassociateWirelessGatewayFromThing	Concede permissão para dissociar uma coisa WirelessGateway de uma coisa do IoT Core	Gravar	WirelessGateway*		iot:DescribeThing
			thing*		
GetDestination	Concede permissão para obter o destino	Leitura	Destination*		
GetDeviceProfile	Concede permissão para obter o DeviceProfile	Leitura	DeviceProfile*		
GetEventConfigurationByResourceTypes	Concede permissão para obter a configuração de evento por tipos de recurso	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetFuotaTask	Concede permissão para obter o FuotaTask	Leitura	FuotaTask*		
GetLogLevelsByResourceTypes	Concede permissão para obter níveis de log por tipos de recurso	Leitura			
GetMetricConfiguration	Concede permissão para obter a configuração de métricas	Leitura			
GetMetrics	Concede permissão para obter métricas	Leitura			
GetMulticastGroup	Concede permissão para obter o MulticastGroup	Leitura	MulticastGroup*		
GetMulticastGroupSession	Concede permissão para obter a MulticastGroup sessão	Leitura	MulticastGroup*		
GetNetworkAnalyzerConfiguration	Concede permissão para obter o NetworkAnalyzerConfiguration	Leitura	NetworkAnalyzerConfiguration*		
GetPartnerAccount	Concede permissão para obter o associado PartnerAccount	Leitura	SidewalkAccount*		
GetPosition	Concede permissão para obter a posição de um determinado recurso	Leitura	WirelessDevice		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			WirelessGateway		
GetPositionConfiguration	Concede permissão para obter a configuração de posição de um determinado recurso	Leitura	WirelessDevice		
			WirelessGateway		
GetPositionEstimate	Concede permissão para obter uma estimativa de posição	Leitura			
GetResourceEventConfiguration	Concede permissão para obter uma configuração de evento para um identificador	Leitura	SidewalkAccount		
			WirelessDevice		
			WirelessGateway		
GetResourceLogLevel	Concede permissão para obter o nível de log do recurso	Leitura	WirelessDevice		
			WirelessGateway		
GetResourcePosition	Concede permissão para obter a posição de um determinado recurso	Leitura	WirelessDevice		
			WirelessGateway		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetServiceEndpoint	Concede permissão para recuperar o endpoint específico da conta do cliente para conexão de protocolo CUPS ou conexão de protocolo LoRaWAN Network Server (LNS) e, opcionalmente, certificado de confiança do servidor no formato PEM	Leitura			
GetServiceProfile	Concede permissão para obter o ServiceProfile	Leitura	ServiceProfile*		
GetWirelessDevice	Concede permissão para obter o WirelessDevice	Leitura	WirelessDevice*		
GetWirelessDeviceImportTask	Concede permissão para obter a tarefa de importação de dispositivos sem fio	Leitura	ImportTask*		
GetWirelessDeviceStatistics	Concede permissão para obter informações estatísticas de um determinado WirelessDevice	Leitura	WirelessDevice*		
GetWirelessGateway	Concede permissão para obter o WirelessGateway	Leitura	WirelessGateway*		
GetWirelessGatewayCertificate	Concede permissão para obter o ID do certificado IoT Core Identity associado ao WirelessGateway	Leitura	WirelessGateway*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetWirelessGatewayFirmwareInformation	Concede permissão para obter a versão atual do firmware e outras informações para o WirelessGateway	Leitura	WirelessGateway*		
GetWirelessGatewayStatistics	Concede permissão para obter informações estatísticas de um determinado WirelessGateway	Leitura	WirelessGateway*		
GetWirelessGatewayTask	Concede permissão para obter a tarefa para um determinado WirelessGateway	Leitura	WirelessGateway*		
GetWirelessGatewayTaskDefinition	Concede permissão para obter a definição de WirelessGateway tarefa fornecida	Leitura	WirelessGatewayTaskDefinition*		
ListDestinations	Concede permissão para listar informações de destinos disponíveis com base no Conta da AWS	Leitura			
ListDeviceProfiles	Concede permissão para listar as informações disponíveis DeviceProfiles com base no Conta da AWS	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDevicesForWirelessDeviceImportTask	Concede permissão para listar informações de dispositivos por tarefa de importação de dispositivos sem fio com base no Conta da AWS	Leitura	ImportTask*		
ListEventConfigurations	Concede permissão para listar informações das configurações de eventos disponíveis com base no Conta da AWS	Leitura			
ListFuotaTasks	Concede permissão para listar as informações disponíveis FuotaTasks com base no Conta da AWS	Leitura			
ListMulticastGroups	Concede permissão para listar as informações disponíveis MulticastGroups com base no Conta da AWS	Leitura			
ListMulticastGroupsByFuotaTask	Concede permissão para listar as informações disponíveis MulticastGroups por FuotaTask com base no Conta da AWS	Leitura	FuotaTask*		
ListNetworkAnalyzerConfigurations	Concede permissão para listar as informações disponíveis NetworkAnalyzerConfigurations com base no Conta da AWS	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListPartnerAccounts	Concede permissão para listar as contas de parceiros disponíveis	Leitura			
ListPositionConfigurations	Concede permissão para listar informações das configurações de posição disponíveis com base no Conta da AWS	Leitura			
ListQueuedMessages	Concede permissão para listar as mensagens na fila	Leitura			
ListServiceProfiles	Concede permissão para listar as informações disponíveis ServiceProfiles com base no Conta da AWS	Leitura			
ListTagsForResource	Concede permissão para listar todas as etiquetas para determinado recurso	Leitura	Destination		
			DeviceProfile		
			FuotaTask		
			ImportTask		
			MulticastGroup		
			NetworkAnalyzerConfiguration		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			ServiceProfile		
			SidewalkAccount		
			WirelessDevice		
			WirelessGateway		
			WirelessGatewayTaskDefinition		
ListWirelessDeviceImportTasks	Concede permissão para listar as informações de tarefas de importação de dispositivos sem fio com base no Conta da AWS	Leitura			
ListWirelessDevices	Concede permissão para listar as informações disponíveis WirelessDevices com base no Conta da AWS	Leitura			
ListWirelessGatewayTaskDefinitions	Concede permissão para listar informações das definições de WirelessGateway tarefas disponíveis com base no Conta da AWS	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListWirelessGateways	Concede permissão para listar as informações disponíveis WirelessGateways com base no Conta da AWS	Leitura			
PutPositionConfiguration	Concede permissão para colocar a configuração de posição de um determinado recurso	Gravar	WirelessDevice		
			WirelessGateway		
PutResourceLogLevel	Concede permissão para colocar o nível de log de recursos	Write	WirelessDevice		
			WirelessGateway		
ResetAllResourceLogLevels	Concede permissão para redefinir todos os níveis de log de recursos	Write			
ResetResourceLogLevel	Concede permissão para redefinir o nível de log de recursos	Gravar	WirelessDevice		
			WirelessGateway		
SendDataToMulticastGroup	Concede permissão para enviar dados para o Multicast Group	Gravar	MulticastGroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SendDataToWirelessDevice	Concede permissão para enviar o quadro de dados da aplicação descriptografado para o dispositivo de destino	Gravar	WirelessDevice*		
StartBulkAssociateWirelessDeviceWithMulticastGroup	Concede permissão para associar o WirelessDevices com MulticastGroup	Gravar	MulticastGroup*		
StartBulkDisassociateWirelessDeviceFromMulticastGroup	Concede permissão para desassociar em massa o formulário WirelessDevices MulticastGroup	Gravar	MulticastGroup*		
StartFuotaTask	Concede permissão para iniciar o FuotaTask	Gravar	FuotaTask*		
StartMulticastGroupSession	Concede permissão para iniciar a MulticastGroup sessão	Gravar	MulticastGroup*		
StartNetworkAnalyzerStream	Concede permissão para iniciar a NetworkAnalyzer transmissão	Gravar	NetworkAnalyzerConfiguration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartSingleWirelessDeviceImportTask	Concede permissão para iniciar a única tarefa de importação de dispositivos sem fio	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
StartWirelessDeviceImportTask	Concede permissão para iniciar a tarefa de importação de dispositivos sem fio	Gravar	ImportTask*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Concede permissão para marcar determinado recurso	Marcação	Destination		
			DeviceProfile		
			FuotaTask		
			ImportTask		
			MulticastGroup		
			NetworkAnalyzerConfiguration		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			ServiceProfile		
			SidewalkAccount		
			WirelessDevice		
			WirelessGateway		
			WirelessGatewayTaskDefinition		
				aws:RequestTag/${TagKey} aws:TagKeys	
TestWirelessDevice	Concede permissão para simular um dispositivo provisionado para enviar dados de uplink com carga útil de "Hello"	Write	WirelessDevice*		
UntagResource	Concede permissão para remover as etiquetas fornecidas do recurso	Marcação	Destination		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			DeviceProfile		
			FuotaTask		
			ImportTask		
			MulticastGroup		
			NetworkAnalyzerConfiguration		
			ServiceProfile		
			SidewalkAccount		
			WirelessDevice		
			WirelessGateway		
			WirelessGatewayTaskDefinition		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateDestination	Concede permissão para atualizar um recurso de destino	Gravar	Destination*		
UpdateEventConfigurationByResourceTypes	Concede permissão para atualizar a configuração de evento por tipos de recurso	Gravar			
UpdateFuotaTask	Concede permissão para atualizar o FuotaTask	Gravar	FuotaTask*		
UpdateLogLevelsByResourceTypes	Concede permissão para atualizar níveis de log por tipos de recurso	Gravar			
UpdateMetricConfiguration	Concede permissão para atualizar uma configuração de métrica	Gravar			
UpdateMulticastGroup	Concede permissão para atualizar o MulticastGroup	Gravar	MulticastGroup*		
UpdateNetworkAnalyzerConfiguration	Concede permissão para atualizar o NetworkAnalyzerConfiguration	Gravar	MulticastGroup*		
			NetworkAnalyzerConfiguration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			WirelessDevice*		
			WirelessGateway*		
UpdatePartnerAccount	Concede permissão para atualizar uma conta de parceiro	Gravar	SidewalkAccount*		
UpdatePosition	Concede permissão para atualizar a posição de um determinado recurso	Gravar	WirelessDevice		
			WirelessGateway		
UpdateResourceEventConfiguration	Concede permissão para atualizar uma configuração de evento para um identificador	Gravar	SidewalkAccount		
			WirelessDevice		
			WirelessGateway		
UpdateResourcePosition	Concede permissão para atualizar a posição de um determinado recurso	Gravar	WirelessDevice		
			WirelessGateway		
UpdateWirelessDevice	Concede permissão para atualizar um WirelessDevice recurso	Gravar	WirelessDevice*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateWirelessDeviceImportTask	Concede permissão para atualizar uma tarefa de importação de dispositivos sem fio	Gravar	ImportTask*		
UpdateWirelessGateway	Concede permissão para atualizar um WirelessGateway recurso	Gravar	WirelessGateway*		

Tipos de recursos definidos pelo AWS IoT Wireless

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Tipos de recursos	ARN	Chaves de condição
ServiceProfile	arn:${Partition}:iotwireless:${Region}:${Account}:ServiceProfile/${ServiceProfileId}	aws:ResourceTag/${TagKey}
Destination	arn:${Partition}:iotwireless:${Region}:${Account}:Destination/${DestinationName}	aws:ResourceTag/${TagKey}
SidewalkAccount	arn:${Partition}:iotwireless:${Region}:${Account}:SidewalkAccount/${SidewalkAccountId}	aws:ResourceTag/${TagKey}
WirelessGatewayTaskDefinition	arn:${Partition}:iotwireless:${Region}:${Account}:WirelessGatewayTaskDefinition/${WirelessGatewayTaskDefinitionId}	aws:ResourceTag/${TagKey}
FuotaTask	arn:${Partition}:iotwireless:${Region}:${Account}:FuotaTask/${FuotaTaskId}	aws:ResourceTag/${TagKey}
MulticastGroup	arn:${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}	

Tipos de recursos	ARN	Chaves de condição
ImportTask	`arn:${Partition}:iotwireless:${Region}:${Account}:ImportTask/${ImportTaskId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS IoT Wireless

AWS O IoT Wireless define as seguintes chaves de condição que podem ser usadas `Condition` no elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso por uma chave da etiqueta que está presente na solicitação que o usuário faz ao IoT Wireless.	String
aws:ResourceTag/${TagKey}	Filtra o acesso por componente chave da etiqueta de uma etiqueta associada a um recurso IoT Wireless	String
aws:TagKeys	Filtra o acesso pela lista de todos os nomes de chave da etiqueta associados ao recurso na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS IQ

AWS O IQ (prefixo do serviço:`iq`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS IQ
- Tipos de recursos definidos pelo AWS IQ
- Chaves de condição do AWS IQ

Ações definidas pelo AWS IQ

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de

condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptCall	Concede permissão para aceitar uma chamada voice/video	Gravar	call*		
ApprovePaymentRequest	Concede permissão para aprovar uma solicitação de pagamento	Gravar	paymentRequest*		
ApproveProposal	Concede permissão para aprovar uma proposta	Gravar	proposal*		
ArchiveConversation	Concede permissão para arquivar uma conversa	Gravar	conversation*		
CompleteProposal	Concede permissão para concluir uma proposta	Gravar	proposal*		
CreateConversation	Concede permissão para responder a uma solicitação ou enviar uma mensagem	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	direta para iniciar uma conversa				
CreateExpert	Concede permissão para criar um perfil de especialista	Gravar			
CreateListing	Concede permissão para criar um anúncio	Gravar			
CreateMilestoneProposal	Concede permissão para criar um proposta de marco	Gravar			
CreatePaymentRequest	Concede permissão para criar uma solicitação de pagamento	Gravar			
CreateProject	Concede permissão para enviar novas solicitações	Gravar			
CreateRequest	Concede permissão para enviar novas solicitações	Gravar			
CreateScheduledProposal	Concede permissão para criar uma proposta agendada	Gravar			
CreateSeller	Concede permissão para criar um perfil de vendedor	Gravar			
CreateUpfrontProposal	Concede permissão para criar uma proposta antecipada	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeclineCall	Concede permissão para recusar uma chamada recebida voice/video	Gravar	call*		
DeleteAttachment	Concede permissão para excluir um anexo existente	Gravar	attachment*		
DisableIndividualPublicProfile	Concede permissão para desativar a página de perfil público individual	Gravar	expert*		
DownloadAttachment	Concede permissão para baixar o anexo existente	Leitura	attachment*		
EnableIndividualPublicProfile	Concede permissão para ativar a página de perfil público individual	Gravar	expert*		
EndCall	Concede permissão para encerrar uma voice/video chamada	Gravar	call*		
GetBuyer	Concede permissão para ler as informações do comprador	Leitura	buyer*		
GetCall	Concede permissão para ler os detalhes de uma voice/video chamada	Leitura	call*		
GetChatInfo	Concede permissão para ler detalhes do ambiente de bate-papo sobre uma conversa	Leitura	conversation*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetChatMessages	Concede permissão para ler mensagens de bate-papo em uma conversa	Leitura	conversation*		
GetChatToken	Concede permissão para solicitar um token de websocket para as notificações de conversas	Leitura	token*		
GetCompanyChatMessages	Concede permissão para ler mensagens de chat em uma conversa da empresa	Leitura	conversation*		
GetCompanyProfile	Concede permissão para ler um perfil de empresa	Leitura	company*		
GetConversation	Concede permissão para ler detalhes de uma conversa	Leitura	conversation*		
GetExpert	Concede permissão para ler as informações do especialista	Leitura	expert*		
GetListing	Concede permissão para ler um anúncio	Leitura	listing*		
GetMarketplaceSeller	Concede permissão para ler as informações de um perfil de vendedor	Leitura	seller*		
GetPaymentRequest	Concede permissão para ler uma solicitação de pagamento	Leitura	paymentRequest*		
GetProposal	Concede permissão para ler uma proposta	Leitura	proposal*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetRequest	Concede permissão para obter uma solicitação criada	Leitura	request*		
GetReview	Concede permissão para ler uma avaliação de um especialista	Leitura	seller*		
HideRequest	Concede permissão para ocultar uma solicitação	Gravar	request*		
InitiateCall	Concede permissão para iniciar uma voice/video chamada	Gravar			
LinkAwsCertification	Concede permissão para vincular uma AWS certificação a um perfil individual	Gravar	expert*		
ListAttachments	Concede permissão para listar anexos existentes	Lista	attachment*		
ListConversations	Concede permissão para listar conversas existentes	Leitura	conversation*		
ListExpertAccessLogs	Concede permissão para listar logs de acesso de atividades de especialistas	Leitura	permission*		
ListListings	Concede permissão para listar anúncios	Leitura	listing*		
ListPaymentRequests	Concede permissão para listar solicitações de pagamento	Leitura	paymentRequest		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			paymentSchedule		
ListProposals	Concede permissão para listar propostas	Leitura	proposal*		
ListRequests	Concede permissão para listar solicitações que são criadas	Leitura	request*		
ListReviews	Concede permissão para listar avaliações de um especialista	Leitura	seller*		
MarkChatMessageRead	Concede permissão para marcar uma mensagem como lida em uma conversa	Gravar	conversation*		
RejectPaymentRequest	Concede permissão para rejeitar uma solicitação de pagamento	Gravar	paymentRequest*		
RejectProposal	Concede permissão para rejeitar uma proposta	Gravar	proposal*		
SendCompanyChatMessage	Concede permissão para enviar uma mensagem em uma conversa como empresa	Gravar	conversation*		
SendIndividualChatMessage	Concede permissão para enviar uma mensagem em uma conversa como pessoa física	Gravar	conversation*		
UnarchiveConversation	Concede permissão para desarquivar uma conversa	Gravar	conversation*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UnlinkAwsCertification	Concede permissão para desvincular uma AWS certificação do perfil individual	Gravar	expert*		
UpdateCompanyProfile	Concede permissão para atualizar um perfil de empresa	Gravar	company*		
UpdateConversationMembers	Concede permissão para adicionar mais participantes a uma conversa	Gravar	conversation*		
UpdateExpert	Concede permissão para atualizar informações de um especialista	Gravar	expert*		
UpdateListing	Concede permissão para atualizar um anúncio	Gravar	listing*		
UpdateRequest	Concede permissão para atualizar uma solicitação	Gravar	request*		
UploadAttachment	Concede permissão para carregar um anexo	Gravar			
WithdrawPaymentRequest	Concede permissão para retirar uma solicitação de pagamento	Gravar	paymentRequest*		
WithdrawProposal	Concede permissão para retirar uma proposta	Gravar	proposal*		
WriteReview	Concede permissão para escrever uma avaliação para um especialista	Gravar	seller*		

Tipos de recursos definidos pelo AWS IQ

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}`	

Tipos de recursos	ARN	Chaves de condição
seller	`arn:${Partition}:iq:${Region}::seller/${SellerAwsAccountId}`	
company	`arn:${Partition}:iq:${Region}::company/${CompanyId}`	
request	`arn:${Partition}:iq:${Region}::request/${RequestId}`	
listing	`arn:${Partition}:iq:${Region}::listing/${ListingId}`	
attachment	`arn:${Partition}:iq:${Region}::attachment/${AttachmentId}`	
permission	`arn:${Partition}:iq-permission:${Region}::permission/${PermissionRequestId}`	

Chaves de condição do AWS IQ

O IQ não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS IQ Permissions

AWS O IQ Permissions (prefixo do serviço:`iq-permission`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS IQ Permissions
- Tipos de recursos definidos pelo AWS IQ Permissions
- Chaves de condição do AWS IQ Permissions

Ações definidas pelo AWS IQ Permissions

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ApproveAccessGrant	Concede permissão para aprovar uma solicitação de permissão	Gravar	permission*		
ApprovePermissionRequest	Concede permissão para aprovar uma solicitação de permissão	Gravar	permission*		
AssumePermissionRole	Concede permissão para obter um conjunto de credenciais de segurança temporárias para especialistas, que eles podem usar para acessar os recursos dos compradores AWS	Gravar	permission*		
CreatePermissionRequest	Concede permissão para criar uma solicitação de permissão	Gravar	permission*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetPermissionRequest	Concede permissão para obter uma solicitação de permissão	Leitura	permission*		
ListPermissionRequests	Concede permissão para listar uma solicitação de permissão	Leitura	permission*		
RejectPermissionRequest	Concede permissão para rejeitar uma solicitação de permissão	Gravar	permission*		
RevokePermissionRequest	Concede permissão para revogar uma solicitação de permissão aprovada anteriormente	Gravar	permission*		
WithdrawPermissionRequest	Concede permissão para retirar uma solicitação de permissão que não foi aprovada ou recusada	Gravar	permission*		

Tipos de recursos definidos pelo AWS IQ Permissions

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
permission	`arn:${Partition}:iq-permission:${Region}::permission/${PermissionRequestId}`	

Chaves de condição do AWS IQ Permissions

A permissão do IQ não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do Amazon Kendra

O Amazon Kendra (prefixo do serviço: `kendra`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Kendra
- Tipos de recursos definidos pelo Amazon Kendra
- Chaves de condição do Amazon Kendra

Ações definidas pelo Amazon Kendra

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateEntitiesToExperience	Concede permissão para colocar o mapeamento principal no índice	Gravar	experience*		
			index*		
AssociatePersonasToEntities	Define as permissões específicas de usuários ou grupos em sua fonte de identidade de AWS SSO com acesso à sua experiência com o Amazon Kendra	Gravar	experience*		
			index*		
BatchDeleteDocument	Concede permissão para excluir documentos em lote	Gravar	index*		
BatchDeleteFeaturedResultsSet	Concede permissão para excluir um conjunto de resultados em destaque	Gravar	featured-results-set*		
			index*		
BatchGetDocumentStatus	Concede permissão para obter o status do documento em lote	Leitura	index*		
BatchPutDocument	Conceder permissão para colocar documento em lote	Gravar	index*		
ClearQuerySuggestions	Concede permissão para limpar as sugestões para um determinado índice gerado até agora	Gravar	index*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAccessControlConfiguration	Concede permissão para criar uma configuração de controle de acesso	Gravar	index*		
CreateDataSource	Concede permissão para criar uma fonte de dados	Gravar	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExperience	Cria uma experiência do Amazon Kendra, como uma aplicação de pesquisa	Gravar	index*		
CreateFaq	Concede permissão para criar uma sessão de perguntas frequentes	Gravar	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFeaturedResultsSet	Concede permissão para criar um conjunto de resultados em destaque	Gravar	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateIndex	Concede permissão para criar um índice	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateQuerySuggestionsBlockList	Concede permissão para criar um QuerySuggestions BlockList	Gravar	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateThesaurus	Concede permissão para criar um léxico	Gravar	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessControlConfiguration	Concede permissão para excluir uma configuração de controle de acesso	Gravar	access-control-configuration*		
			index*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteDataSource	Concede permissão para excluir uma fonte de dados	Gravar	data-source*		
			index*		
DeleteExperience	Exclui sua experiência do Amazon Kendra, como uma aplicação de pesquisa	Gravar	experience*		
			index*		
DeleteFaq	Concede permissão para excluir uma seção de perguntas frequentes	Gravar	faq*		
			index*		
DeleteIndex	Concede permissão para excluir um índice	Gravar	index*		
DeletePrincipalMapping	Concede permissão para excluir o mapeamento principal do índice	Gravar	index*		
			data-source		
DeleteQuerySuggestionsBlockList	Concede permissão para excluir um QuerySuggestions BlockList	Gravar	index*		
			query-suggestions-block-list*		
DeleteThesaurus	Concede permissão para excluir um léxico	Gravar	index*		
			thesaurus*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeAccessControlConfiguration	Concede permissão para descrever uma configuração de controle de acesso	Leitura	access-control-configuration*		
			index*		
DescribeDataSource	Concede permissão para descrever uma fonte de dados	Leitura	data-source*		
			index*		
DescribeExperience	Obtém informações sobre a sua experiência do Amazon Kendra, como uma aplicação de pesquisa	Leitura	experience*		
			index*		
DescribeFaq	Concede permissão para descrever uma seção de perguntas frequentes	Leitura	faq*		
			index*		
DescribeFeaturedResultsSet	Concede permissão para descrever um conjunto de resultados em destaque	Leitura	featured-results-set*		
			index*		
DescribeIndex	Concede permissão para descrever um índice	Leitura	index*		
DescribePrincipalMapping	Concede permissão para descrever o mapeamento principal do índice	Leitura	index*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			data-source		
DescribeQuerySuggestionsBlockList	Concede permissão para descrever um QuerySuggestions BlockList	Leitura	index*		
			query-suggestions-block-list*		
DescribeQuerySuggestionsConfig	Concede permissão para descrever a configuração de sugestões de consulta para um índice	Leitura	index*		
DescribeThesaurus	Concede permissão para descrever um léxico	Leitura	index*		
			thesaurus*		
DisassociateEntitiesFromExperience	Impede que usuários ou grupos em sua fonte de identidade de AWS SSO acessem sua experiência com o Amazon Kendra	Gravar	experience*		
			index*		
DisassociatePersonasFromEntities	Remove as permissões específicas de usuários ou grupos em sua fonte de identidade de AWS SSO com acesso à sua experiência com o Amazon Kendra	Gravar	experience*		
			index*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetQuerySuggestions	Concede permissão para obter sugestões para um prefixo de consulta	Leitura	index*		
GetSnapshots	Recupera dados de métricas de pesquisa	Leitura	index*		
ListAccessControlConfigurations	Concede permissão para listar as configurações de controle de acesso	Lista	index*		
ListDataSourceSyncJobs	Concede permissão para obter histórico de trabalho de sincronização de origem dos dados	Lista	data-source*		
			index*		
ListDataSources	Concede permissão para listar as origens de dados	Lista	index*		
ListEntityPersonas	Lista permissões específicas de usuários e grupos com acesso à sua experiência do Amazon Kendra	Lista	experience*		
			index*		
ListExperienceEntities	Lista usuários ou grupos em sua fonte de identidade de AWS SSO que têm acesso concedido à sua experiência com o Amazon Kendra	Lista	experience*		
			index*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListExperiences	Lista uma ou mais experiências do Amazon Kendra. Você pode criar uma experiência do Amazon Kendra, como uma aplicação de pesquisa	Lista	index*		
ListFaqs	Concede permissão para listar as perguntas frequentes	Lista	index*		
ListFeaturedResultsSets	Concede permissão para listar os conjuntos de resultados em destaque	Lista	index*		
ListGroupsOlderThanOrderingId	Concede permissão para listar os grupos que são mais antigos do que um ID de pedido	Lista	index*		
			data-source		
ListIndices	Concede permissão para listar os índices	Lista			
ListQuerySuggestionsBlockLists	Concede permissão para listar o QuerySuggestions BlockLists	Lista	index*		
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	data-source		
			faq		
			featured-results-set		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			index		
			query-suggestions-block-list		
			thesaurus		
ListThesauri	Concede permissão para listar o léxico	Lista	index*		
PutPrincipalMapping	Concede permissão para colocar o mapeamento principal no índice	Gravar	index*		
			data-source		
Query	Concede permissão para consultar documentos e perguntas frequentes	Leitura	index*		
Retrieve	Concede permissão para recuperar conteúdo relevante de um índice	Leitura	index*		
StartDataSourceSyncJob	Concede permissão para iniciar o trabalho de sincronização de origem dos dados	Gravar	data-source*		
			index*		
StopDataSourceSyncJob	Concede permissão para interromper o trabalho de sincronização de origem dos dados	Gravar	data-source*		
			index*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SubmitFeedback	Concede permissão para enviar comentários sobre os resultados de uma consulta	Gravar	index*		
TagResource	Concede permissão para marcar um recurso com determinados pares de chave-valor	Tags	data-source		
			faq		
			featured-results-set		
			index		
			query-suggestions-block-list		
			thesaurus		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover a etiqueta com a chave fornecida de um recurso	Tags	data-source		
			faq		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			featured-results-set		
			index		
			query-suggestions-block-list		
			thesaurus		
				aws:TagKeys	
UpdateAccessControlConfiguration	Concede permissão para atualizar uma configuração de controle de acesso	Gravar	access-control-configuration*		
			index*		
UpdateDataSource	Concede permissão para atualizar uma fonte de dados	Gravar	data-source*		
			index*		
UpdateExperience	Atualiza sua experiência do Amazon Kendra, como uma aplicação de pesquisa	Gravar	index*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateFeaturedResultsSet	Concede permissão para atualizar um conjunto de resultados em destaque	Gravar	featured-results-set*		
			index*		
UpdateIndex	Concede permissão para atualizar um índice	Gravar	index*		
UpdateQuerySuggestionsBlockList	Concede permissão para atualizar um QuerySuggestions BlockList	Gravar	index*		
			query-suggestions-block-list*		
UpdateQuerySuggestionsConfig	Concede permissão para atualizar a configuração de sugestões de consulta para um índice	Gravar	index*		
UpdateThesaurus	Concede permissão para atualizar um léxico	Gravar	index*		
			thesaurus*		

Tipos de recursos definidos pelo Amazon Kendra

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves

são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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/${TagKey}
experience	arn:${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}	

Chaves de condição do Amazon Kendra

O Amazon Kendra define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o Amazon Kendra Intelligent Ranking

O Amazon Kendra Intelligent Ranking (prefixo de serviço: `kendra-ranking`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Kendra Intelligent Ranking
- Tipos de recursos definidos pelo Amazon Kendra Intelligent Ranking
- Chaves de condição para o Amazon Kendra Intelligent Ranking

Ações definidas pelo Amazon Kendra Intelligent Ranking

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de

recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateRescoreExecutionPlan	Concede permissão para criar um RescoreExecutionPlan	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteRescoreExecutionPlan	Concede permissão para excluir um RescoreExecutionPlan	Gravar	rescore-execution-plan*		
DescribeRescoreExecutionPlan	Concede permissão para descrever um RescoreExecutionPlan	Leitura	rescore-execution-plan*		
ListRescoreExecutionPlans	Concede permissão para listar tudo RescoreExecutionPlans	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	rescore-execution-plan		
Rescore	Concede permissão para reclassificar documentos com o Kendra Intelligent Ranking	Leitura	rescore-execution-plan*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para marcar um recurso com determinados pares de chave-valor	Tags	rescore-execution-plan		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover a etiqueta com a chave fornecida de um recurso	Tags	rescore-execution-plan		
				aws:TagKeys	
UpdateRescoreExecutionPlan	Concede permissão para atualizar um RescoreExecutionPlan	Gravar	rescore-execution-plan*		

Tipos de recursos definidos pelo Amazon Kendra Intelligent Ranking

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
rescore-execution-plan	`arn:${Partition}:kendra-ranking:${Region}:${Account}:rescore-execution-plan/${RescoreExecutionPlanId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o Amazon Kendra Intelligent Ranking

O Amazon Kendra Intelligent Ranking define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Keyspaces (for Apache Cassandra)

O Amazon Keyspaces (for Apache Cassandra) (prefixo do serviço: `cassandra`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Keyspaces (for Apache Cassandra)
- Tipos de recursos definidos pelos Amazon Keyspaces (for Apache Cassandra)
- Chaves de condição do Amazon Keyspaces (for Apache Cassandra)

Ações definidas pelo Amazon Keyspaces (for Apache Cassandra)

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
Alter	Concede permissão para alterar um espaço de chave ou uma tabela	Gravar	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
AlterMultiRegionResource	Concede permissão para alterar um espaço de chave ou tabela multirregional	Gravar	keyspace		
			table		
				aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
Create	Concede permissão para criar um espaço de chave ou uma tabela	Gravar	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMultiRegionResource	Concede permissão para criar um espaço de chave ou tabela multirregional	Gravar	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
Drop	Concede permissão para remover um espaço de chave ou uma tabela	Gravar	keyspace		
			table		
DropMultiRegionResource	Concede permissão para descartar um espaço de chave ou tabela multirregional	Gravar	keyspace		
			table		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetRecords	Concede permissão para recuperar os registros de stream do CDC de um determinado fragmento	Leitura	stream*		
GetShardIterator	Concede permissão para retornar um iterador de fragmento	Leitura	stream*		
GetStream	Concede permissão para retornar informações sobre um fluxo do CDC, incluindo a composição de seus fragmentos	Leitura	stream*		
ListStreams	Concede permissão para retornar uma matriz de fluxo CDC ARNs associada à conta atual e ao endpoint	Lista			
Modify	Concede permissão para INSERT (inserir), UPDATE (atualizar) ou DELETE (excluir) dados em uma tabela	Gravar	table*		
ModifyMultiRegionResource	Concede permissão para INSERT (inserir), UPDATE (atualizar) ou DELETE (excluir) dados em uma tabela multirregional	Gravar	table*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
Restore	Concede permissão para restaurar a tabela de um backup	Gravar	table*		
RestoreMultiRegionTable	Concede permissão para restaurar a tabela multirregional de um backup	Gravar	table*		
Select	Concede permissão para SELECT (selecionar) dados de uma tabela	Leitura	table*		
SelectMultiRegionResource	Concede permissão para SELECT dados de uma tabela multirregional	Leitura	table*		
TagMultiRegionResource	Concede permissão para marcar um espaço de chave ou tabela multirregional	Tags	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Concede permissão para marcar um keyspace, tabela ou stream	Tags	keyspace		
			stream		
			table		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UnTagMultiRegionResource	Concede permissão para desmarcar um espaço de chave ou tabela multirregional	Tags	keyspace		
			table		
				aws:TagKeys	
UntagResource	Concede permissão para desmarcar um keyspace, tabela ou stream	Tags	keyspace		
			stream		
			table		
				aws:TagKeys	
UpdatePartitioner	Concede permissão para ATUALIZAR o particionador em uma tabela do sistema	Gravar	table*		

Tipos de recursos definidos pelos Amazon Keyspaces (for Apache Cassandra)

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves

são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do Amazon Keyspaces (for Apache Cassandra)

O Amazon Keyspaces (for Apache Cassandra) define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base na presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra ações com base nos pares de chave-valor da etiqueta anexados ao recurso	String

Chaves de condição	Descrição	Type
aws:TagKeys	Filtra ações com base na presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Kinesis Analytics

O Amazon Kinesis Analytics (prefixo do serviço: `kinesisanalytics`) fornece os seguintes recursos, ações e chaves de contexto de condição para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Kinesis Analytics
- Tipos de recursos definidos pelo Amazon Kinesis Analytics
- Chaves de condição do Amazon Kinesis Analytics

Ações definidas pelo Amazon Kinesis Analytics

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddApplicationInput	Concede permissão para adicionar entrada à aplicação	Gravar	application*		
AddApplicationOutput	Concede permissão para adicionar saída à aplicação	Write	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddApplicationReferenceDataSource	Concede permissão para adicionar fonte de dados de referência à aplicação	Gravar	application*		
CreateApplication	Concede permissão para criar um aplicativo	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Concede permissão para excluir uma aplicação	Gravar	application*		
DeleteApplicationOutput	Concede permissão para excluir a saída especificada da aplicação	Write	application*		
DeleteApplicationReferenceDataSource	Concede permissão para excluir a fonte de dados de referência especificada da aplicação	Gravar	application*		
DescribeApplication	Concede permissão para descrever a aplicação especificada	Leitura	application*		
DiscoverInputSchema	Concede permissão para descobrir o esquema de entrada para a aplicação	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetApplicationState [somente permissão]	Concede permissão ao console do Kinesis Data Analytics para exibir resultados de fluxo para aplicações de runtime SQL do Kinesis Data Analytics	Leitura	application*		
ListApplications	Concede permissão para listar as aplicações para a conta	List			
ListTagsForResource	Concede permissão para obter as etiquetas associadas à aplicação	Read	application*		
StartApplication	Concede permissão para iniciar a aplicação	Write	application*		
StopApplication	Concede permissão para interromper a aplicação	Write	application*		
TagResource	Concede permissão para adicionar etiquetas à aplicação	Marcação	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover as etiquetas especificadas da aplicação	Marcação	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
UpdateApplication	Concede permissão para atualizar uma aplicação	Gravar	application*		

Tipos de recursos definidos pelo Amazon Kinesis Analytics

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
application	`arn:${Partition}:kinesisanalytics:${Region}:${Account}:application/${ApplicationName}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Kinesis Analytics

O Amazon Kinesis Analytics define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por conjunto de valores para cada uma das tags	String
aws:ResourceTag/${TagKey}	Filtra o acesso por valor-tag associado ao recurso	String
aws:TagKeys	Filtra o acesso pela presença de chaves de tag obrigatórias na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Kinesis Analytics V2

O Amazon Kinesis Analytics V2 (prefixo do serviço: `kinesisanalytics`) fornece os seguintes recursos, ações e chaves de contexto de condição para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Kinesis Analytics V2
- Tipos de recursos definidos pelo Amazon Kinesis Analytics V2
- Chaves de condição do Amazon Kinesis Analytics V2

Ações definidas pelo Amazon Kinesis Analytics V2

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddApplicationCloudWatchLoggingOption	Concede permissão para adicionar a opção de registro em log do CloudWatch à aplicação	Write	application*		
AddApplicationInput	Concede permissão para adicionar entrada à aplicação	Write	application*		
AddApplicationInputProcessingConfiguration	Concede permissão para adicionar configuração de processamento de entrada à aplicação	Write	application*		
AddApplicationOutput	Concede permissão para adicionar saída à aplicação	Write	application*		
AddApplicationReferenceDataSource	Concede permissão para adicionar fonte de dados de referência à aplicação	Write	application*		
AddApplicationVpcConfiguration	Concede permissão para adicionar a configuração da VPC à aplicação	Write	application*		
CreateApplication	Concede permissão para criar um aplicativo	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateApplicationPresignedUrl	Concede permissão para criar e retornar um URL que você pode usar para se conectar à extensão de uma aplicação	Read	application*		
CreateApplicationSnapshot	Concede permissão para criar um snapshot para uma aplicação	Write	application*		
DeleteApplication	Concede permissão para excluir uma aplicação	Write	application*		
DeleteApplicationCloudWatchLoggingOption	Concede permissão para excluir a opção de registro em log do CloudWatch especificada à aplicação	Write	application*		
DeleteApplicationInputProcessingConfiguration	Concede permissão para excluir a configuração de processamento de entrada especificada da aplicação	Write	application*		
DeleteApplicationOutput	Concede permissão para excluir a saída especificada da aplicação	Write	application*		
DeleteApplicationReferenceDataSource	Concede permissão para excluir a fonte de dados de referência especificada da aplicação	Write	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteApplicationSnapshot	Concede permissão para excluir um snapshot de uma aplicação	Write	application*		
DeleteApplicationVpcConfiguration	Concede permissão para excluir a configuração de VPC especificada da aplicação	Write	application*		
DescribeApplication	Concede permissão para descrever a aplicação especificada	Leitura	application*		
DescribeApplicationOperation	Concede permissão para descrever a operação de uma aplicação de uma aplicação	Leitura	application*		
DescribeApplicationSnapshot	Concede permissão para descrever o snapshot de uma aplicação	Leitura	application*		
DescribeApplicationVersion	Concede permissão para descrever a versão de aplicativo de um aplicativo	Leitura	application*		
DiscoverInputSchema	Concede permissão para descobrir o esquema de entrada para a aplicação	Leitura			iam:PassRole
ListApplicationOperations	Concede permissão para listar operações de aplicação de uma aplicação	Leitura	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListApplicationSnapshots	Concede permissão para listar os snapshots de uma aplicação	Leitura	application*		
ListApplicationVersions	Concede permissão para listar a versão de aplicativo de um aplicativo	Leitura	application*		
ListApplications	Concede permissão para listar as aplicações para a conta	List			
ListTagsForResource	Concede permissão para obter as etiquetas associadas à aplicação	Leitura	application*		
RollbackApplication	Concede permissão para executar a operação de reversão em um aplicativo	Gravar	application*		
StartApplication	Concede permissão para iniciar a aplicação	Write	application*		
StopApplication	Concede permissão para interromper a aplicação	Write	application*		
TagResource	Concede permissão para adicionar etiquetas à aplicação	Marcação	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para remover as etiquetas especificadas da aplicação	Marcação	application*		
				aws:TagKeys	
UpdateApplication	Concede permissão para atualizar uma aplicação	Gravar	application*		
UpdateApplicationMaintenanceConfiguration	Concede permissão para atualizar a configuração de manutenção de um aplicativo	Gravar	application*		

Tipos de recursos definidos pelo Amazon Kinesis Analytics V2

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
application	`arn:${Partition}:kinesisanalytics:${Region}:${Account}:application/${ApplicationName}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Kinesis Analytics V2

O Amazon Kinesis Analytics V2 define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por conjunto de valores para cada uma das tags	String
aws:ResourceTag/${TagKey}	Filtra o acesso por valor-tag associado ao recurso	String
aws:TagKeys	Filtra o acesso pela presença de chaves de tag obrigatórias na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Kinesis Data Streams

O Amazon Kinesis Data Streams (prefixo do serviço: `kinesis`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Kinesis Data Streams
- Tipos de recursos definidos pelo Amazon Kinesis Data Streams

- Chaves de condição do Amazon Kinesis Data Streams

Ações definidas pelo Amazon Kinesis Data Streams

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddTagsToStream	Concede permissões para adicionar ou atualizar etiquetas para a transmissão do Amazon Kinesis específica. Cada stream pode ter até 50 tags	Tags	stream*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
CreateStream	Concede permissão para criar uma transmissão de vídeo do Amazon Kinesis	Gravar	stream*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
DecreaseStreamRetentionPeriod	Concede permissão para reduzir o período de retenção da transmissão, que é o período em que os registros de dados ficam acessíveis	Gravar	stream*	aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	depois de serem adicionados à transmissão				
DeleteResourcePolicy	Concede permissão para excluir uma política de recursos associada a um stream ou consumidor especificado	Gravar	consumer*	aws:ResourceTag/${TagKey}	
			stream*	aws:ResourceTag/${TagKey}	
DeleteStream	Concede permissão para excluir uma transmissão e todos os seus fragmentos e dados	Gravar	stream*	aws:ResourceTag/${TagKey}	
DeregisterStreamConsumer	Concede permissão para cancelar o registro de um consumidor de transmissão com um fluxo de dados do Kinesis	Gravar	consumer*	aws:ResourceTag/${TagKey}	
DescribeLimits	Concede permissão para descrever os limites do fragmento e o uso da conta	Leitura			
DescribeStream	Concede permissão para descrever a transmissão especificada	Leitura	stream*	aws:ResourceTag/${TagKey}	
DescribeStreamConsumer	Concede permissão para obter a descrição de um consumidor de transmissão registrado	Leitura	consumer*	aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeStreamSummary	Concede permissão para fornecer uma descrição resumida do fluxo de dados do Kinesis especificado sem a lista de fragmentos	Leitura	stream*	aws:ResourceTag/${TagKey}	
DisableEnhancedMonitoring	Concede permissão para desabilitar o monitoramento aprimorado	Gravar			
EnableEnhancedMonitoring	Concede permissão para habilitar o monitoramento aprimorado do fluxo de dados do Kinesis para métricas em nível de fragmentos	Gravar			
GetRecords	Concede permissão para obter registros de dados de um fragmento	Leitura	stream*	aws:ResourceTag/${TagKey}	
GetResourcePolicy	Concede permissão para obter uma política de recursos associada a um stream ou consumidor especificado	Leitura	consumer*	aws:ResourceTag/${TagKey}	
			stream*	aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetShardIterator	Concede permissão para obter um iterador de fragmento. Um iterador de fragmentos expira cinco minutos depois que for retornado ao solicitante	Leitura	stream*	aws:ResourceTag/${TagKey}	
IncreaseStreamRetentionPeriod	Concede permissão para aumentar o período de retenção da transmissão, que é o período em que os registros de dados ficam acessíveis depois de serem adicionados à transmissão	Gravar	stream*	aws:ResourceTag/${TagKey}	
ListShards	Concede permissão para listar os fragmentos em uma transmissão e fornece informações sobre cada fragmento	Lista	stream*	aws:ResourceTag/${TagKey}	
ListStreamConsumers	Concede permissão para listar os consumidores de transmissão registrados para receber dados de uma transmissão do Kinesis usando a distribuição avançada e fornece informações sobre cada consumidor	Lista	stream*	aws:ResourceTag/${TagKey}	
ListStreams	Concede permissões para listar suas transmissões	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar as tags do recurso Amazon Kinesis especificado	Leitura	consumer*	aws:ResourceTag/${TagKey}	
			stream*	aws:ResourceTag/${TagKey}	
ListTagsForStream	Concede permissões para listar as etiquetas para a transmissão do Amazon Kinesis	Leitura	stream*	aws:ResourceTag/${TagKey}	
MergeShards	Concede permissão para mesclar dois fragmentos adjacentes em uma transmissão e combina-os em um único fragmento para reduzir a capacidade da transmissão de ingerir e transportar dados	Gravar	stream*	aws:ResourceTag/${TagKey}	
PutRecord	Concede permissão para gravar um único registro de dados de um produtor em uma transmissão do Amazon Kinesis	Gravar	stream*	aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutRecords	Concede permissão para gravar vários registros de dados de um produtor em um stream do Amazon Kinesis em uma única chamada (também chamada de solicitação) PutRecords	Gravar	stream*	aws:ResourceTag/${TagKey}	
PutResourcePolicy	Concede permissão para anexar uma política de recursos a um stream ou consumidor especificado	Gravar	consumer*	aws:ResourceTag/${TagKey}	
			stream*	aws:ResourceTag/${TagKey}	
RegisterStreamConsumer	Concede permissão para registrar um consumidor de transmissão com um fluxo de dados do Kinesis	Gravar	stream*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RemoveTagsFromStream	Concede permissão para remover etiquetas do fluxo de dados Kinesis especificado. As etiquetas removidas são excluídas e não poderão ser recuperadas depois que essa operação for concluída com êxito	Tags	stream*	aws:TagKeys aws:ResourceTag/${TagKey}	
SplitShard	Concede permissão para dividir um fragmento em dois novos fragmentos no fluxo de dados do Kinesis, a fim de aumentar a capacidade da transmissão de ingerir e transportar dados	Gravar	stream*	aws:ResourceTag/${TagKey}	
StartStreamEncryption	Concede permissão para ativar ou atualizar a criptografia do lado do servidor usando uma chave AWS KMS para um fluxo especificado	Gravar	kmsKey*		
			stream*	aws:ResourceTag/${TagKey}	
StopStreamEncryption	Concede permissão para desabilitar a criptografia no lado do servidor para uma transmissão especificada	Gravar	kmsKey*		
			stream*	aws:ResourceTag/${TagKey}	
SubscribeToShard	Concede permissão para escutar um fragmento específico com distribuição avançada	Leitura	consumer*	aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para adicionar ou atualizar tags para o recurso especificado do Amazon Kinesis. Cada recurso pode ter até 50 tags	Tags	consumer*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			stream*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permissão para remover tags do recurso de dados do Kinesis especificado. As etiquetas removidas são excluídas e não poderão ser recuperadas depois que essa operação for concluída com êxito	Tags	consumer*	aws:TagKeys aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			stream*	aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateShardCount	Concede permissão para atualizar a contagem de fragmentos da transmissão especificada para o número de fragmentos especificados	Gravar			
UpdateStreamMode	Concede permissão para atualizar o modo de capacidade da transmissão de dados	Gravar			

Tipos de recursos definidos pelo Amazon Kinesis Data Streams

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
stream	`arn:${Partition}:kinesis:${Region}:${Account}:stream/${StreamName}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
consumer	`arn:${Partition}:kinesis:${Region}:${Account}:${StreamType}/${StreamName}/consumer/${ConsumerName}:${ConsumerCreationTimpstamp}`	
kmsKey	`arn:${Partition}:kms:${Region}:${Account}:key/${KeyId}`	

Chaves de condição do Amazon Kinesis Data Streams

O Amazon Kinesis Data Streams define as chaves de condição a seguir que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Kinesis Firehose

O Amazon Kinesis Firehose (prefixo do serviço: `firehose`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Kinesis Firehose
- Tipos de recursos definidos pelo Amazon Kinesis Firehose
- Chaves de condição do Amazon Kinesis Firehose

Ações definidas pelo Amazon Kinesis Firehose

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDeliveryStream	Concede permissão para criar um fluxo de entrega	Gravar	deliverystream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDeliveryStream	Concede permissão para excluir um delivery stream e seus dados	Write	deliverystream*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeDeliveryStream	Concede permissão para descrever o delivery stream especificado e obtém o status	Leitura	deliverystream*		
ListDeliveryStreams	Concede permissão para listar seus fluxos de entrega	Lista			
ListTagsForDeliveryStream	Concede permissão para listar as etiquetas para o fluxo de entrega especificado	Lista	deliverystream*		
PutRecord	Concede permissão para gravar um único registro de dados em um fluxo de entrega do Amazon Kinesis Firehose	Gravar	deliverystream*		
PutRecordBatch	Concede permissão para gravar vários registros de dados em um fluxo de entrega em uma única chamada, o que pode atingir uma throughput mais alta por produtor do que ao gravar registros únicos	Gravar	deliverystream*		
StartDeliveryStreamEncryption	Concede permissão para habilitar a criptografia do lado do servidor (SSE) para o fluxo de entrega	Gravar	deliverystream*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopDeliveryStreamEncryption	Concede permissão para desabilitar o destino especificado do fluxo de entrega especificado	Gravar	deliverystream*		
TagDeliveryStream	Concede permissão para adicionar ou atualizar etiquetas para o fluxo de entrega especificado	Tags	deliverystream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagDeliveryStream	Concede permissão para remover etiquetas do fluxo de entrega especificado	Tags	deliverystream*		
				aws:TagKeys	
UpdateDestination	Concede permissão para atualizar o destino especificado do fluxo de entrega especificado	Gravar	deliverystream*		

Tipos de recursos definidos pelo Amazon Kinesis Firehose

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves

são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
deliverystream	`arn:${Partition}:firehose:${Region}:${Account}:deliverystream/${DeliveryStreamName}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Kinesis Firehose

O Amazon Kinesis Firehose define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Kinesis Video Streams

O Amazon Kinesis Video Streams (prefixo do serviço: `kinesisvideo`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Kinesis Video Streams
- Tipos de recursos definidos pelo Amazon Kinesis Video Streams
- Chaves de condição do Amazon Kinesis Video Streams

Ações definidas pelo Amazon Kinesis Video Streams

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ConnectAsMaster	Concede permissão para se conectar como mestre ao canal de sinalização especificado pelo endpoint	Write	channel*		
ConnectAsViewer	Concede permissão para se conectar como visualizador ao canal de sinalização especificado pelo endpoint	Write	channel*		
	Concede permissão para criar um canal de sinalização	Write	channel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSignalingChannel				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStream	Concede permissão para criar um streaming de vídeo do Kinesis	Gravar	stream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteEdgeConfiguration	Concede permissão para excluir a configuração de borda do seu Kinesis Video Stream	Gravar	stream*		
DeleteSignalingChannel	Concede permissão para excluir um canal de sinalização existente	Write	channel*		
DeleteStream	Concede permissão para excluir um streaming de vídeo existente do Kinesis	Gravar	stream*		
DescribeEdgeConfiguration	Concede permissão para descrever a configuração de borda do seu fluxo de vídeo do Kinesis	Leitura	stream*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeImageGenerationConfiguration	Concede permissão para descrever a configuração de geração de imagem do fluxo de vídeo do Kinesis	Leitura	stream*		
DescribeMappedResourceConfiguration	Concede permissão para descrever o recurso mapeado para o streaming de vídeo do Kinesis	Lista	stream*		
DescribeMediaStorageConfiguration	Concede permissão para descrever a configuração de armazenamento de mídia de um canal de sinalização	Leitura	channel*		
DescribeNotificationConfiguration	Concede permissão para descrever a configuração de notificação do fluxo de vídeo do Kinesis	Leitura	stream*		
DescribeSignalingChannel	Concede permissão para descrever o canal de sinalização especificado	List	channel*		
DescribeStream	Concede permissão para descrever o streaming de vídeo especificado do Kinesis	List	stream*		
GetClip	Concede permissão para obter um clipe de mídia de um streaming de vídeo	Read	stream*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetDASHStreamingSessionURL	Concede permissão para criar um URL para streaming de vídeo MPEG-DASH	Read	stream*		
GetDataEndpoint	Concede permissão para obter um endpoint de um streaming especificado para ler ou gravar dados de mídia no Kinesis Video Streams	Read	stream*		
GetHLSStreamingSessionURL	Concede permissão para criar um URL para streaming de vídeo HLS	Read	stream*		
GetIceServerConfig	Concede permissão para obter a configuração do servidor ICE	Leitura	channel*		
GetImages	Concede permissão para obter imagens geradas pelo fluxo de vídeo do Kinesis	Leitura	stream*		
GetMedia	Concede permissão para retornar conteúdo de mídia de um streaming de vídeo do Kinesis	Read	stream*		
GetMediaForFragmentList	Concede permissão para ler e retornar dados de mídia somente do armazenamento persistente	Read	stream*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSignalingChannelEndpoint	Concede permissão para obter endpoints para uma combinação especificada de protocolo e função para um canal de sinalização	Leitura	channel*		
JoinStorageSession	Concede permissão para participar de uma sessão de armazenamento de um canal	Gravar	channel*		
JoinStorageSessionAsViewer	Concede permissão para participar de uma sessão de armazenamento de um canal como visualizador	Gravar	channel*		
ListEdgeAgentConfigurations	Concede permissão para listar configurações de um agente de borda	Lista			
ListFragments	Concede permissão para listar os fragmentos do armazenamento de arquivos com base no token de paginação ou no tipo de seletor com o intervalo especificado.	List	stream*		
ListSignalingChannels	Concede permissão para listar seus canais de sinalização	List			
ListStreams	Concede permissão para listar seus Kinesis Video Streams	List			
ListTagsForResource		Read	channel		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	Concede permissão para obter as etiquetas associadas ao seu recurso		stream		
ListTagsForStream	Concede permissão para buscar as etiquetas associadas ao streaming de vídeo do Kinesis	Read	stream*		
PutMedia	Concede permissão para enviar dados de mídia para um streaming de vídeo do Kinesis	Write	stream*		
SendAlexaOfferToMaster	Concede permissão para enviar a oferta SDP do aplicativo Alexa para o mestre	Gravar	channel*		
StartEdgeConfigurationUpdate	Concede permissão para iniciar a atualização da configuração de borda do seu fluxo de vídeo do Kinesis	Gravar	stream*		
TagResource	Concede permissão para anexar conjuntos de etiquetas ao seu recurso	Marcação	channel		
			stream		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagStream	Concede permissão para anexar conjuntos de etiquetas aos Kinesis Video Streams	Marcação	stream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover uma ou mais etiquetas de um recurso	Marcação	channel		
			stream		
				aws:TagKeys	
UntagStream	Concede permissão para remover uma ou mais etiquetas de seus Kinesis Video Streams	Marcação	stream*		
				aws:TagKeys	
UpdateDataRetention	Concede permissão para atualizar o período de retenção de dados do streaming de vídeo do Kinesis	Gravar	stream*		
UpdateImageGenerationConfiguration	Concede permissão para atualizar a configuração de geração de imagem do fluxo de vídeo do Kinesis	Gravar	stream*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateMediaStorageConfiguration	Concede permissão para criar ou atualizar um mapeamento entre um streaming e um canal de sinalização	Gravar	channel*		
UpdateNotificationConfiguration	Concede permissão para atualizar a configuração de notificação do fluxo de vídeo do Kinesis	Gravar	stream*		
UpdateSignalingChannel	Concede permissão para atualizar um canal de sinalização existente	Write	channel*		
UpdateStream	Concede permissão para atualizar um streaming de vídeo existente do Kinesis	Write	stream*		

Tipos de recursos definidos pelo Amazon Kinesis Video Streams

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
stream	`arn:${Partition}:kinesisvideo:${Region}:${Account}:stream/${StreamName}/${CreationTime}`	aws:ResourceTag/${TagKey}
channel	`arn:${Partition}:kinesisvideo:${Region}:${Account}:channel/${ChannelName}/${CreationTime}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Kinesis Video Streams

O Amazon Kinesis Video Streams define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra solicitações com base no conjunto de valores permitido para cada uma das etiquetas	String
aws:ResourceTag/${TagKey}	Filtra ações com base na etiqueta-valor associada ao fluxo	String
aws:TagKeys	Filtra solicitações com base na presença de chaves da etiqueta obrigatórias na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Lake Formation

AWS Lake Formation (prefixo do serviço:`lakeformation`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Lake Formation
- Tipos de recursos definidos pelo AWS Lake Formation
- Chaves de condição do AWS Lake Formation

Ações definidas pelo AWS Lake Formation

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddLFTagsToResource	Concede permissão para anexar etiquetas do Lake Formation a recursos de catálogo	Tags			
BatchGrantPermissions	Concede permissão para permissões de data lake a um ou mais primários em um lote	Gerenciamento de permissões			
BatchRevokePermissions	Concede permissão para revogar permissões de data	Gerenciamento de			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	lake a um ou mais primários em um lote	permissões			
CancelTransaction	Concede permissão para cancelar a transação específica	Gravar			
CommitTransaction	Concede permissão para confirmar a transação específica	Gravar			
CreateDataCellsFilter	Concede permissão para criar um filtro de célula de dados do Lake Formation	Gravar			
CreateLFTag	Concede permissão para criar uma etiqueta do Lake Formation	Gravar			
CreateLFTagExpression	Concede permissão para criar uma expressão de tag Lake Formation	Gravar			
CreateLakeFormationIdentityCenterConfiguration	Concede permissão para criar uma conexão com o Centro de Identidade do IAM com o Lake Formation para permitir que usuários e grupos do Centro de Identidade do IAM acessem os recursos do catálogo de dados	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateLakeFormationOptIn	Concede permissão para impor permissões do Lake Formation para bancos de dados, tabelas e entidades principais fornecidos	Gravar			
DeleteDataCellsFilter	Concede permissão para excluir um filtro de célula de dados do Lake Formation	Gravar			
DeleteLFTag	Concede permissão para excluir uma etiqueta do Lake Formation	Gravar			
DeleteLFTagExpression	Concede permissão para excluir uma expressão do Lake Formation	Gravar			
DeleteLakeFormationIdentityCenterConfiguration	Concede permissão para excluir uma conexão do Centro de Identidade do IAM com o Lake Formation	Gravar			
DeleteLakeFormationOptIn	Concede permissão para remover a imposição de permissões do Lake Formation dos bancos de dados, tabelas e entidades principais fornecidos	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteObjectsOnCancel	Concede permissão para excluir os objetos especificados se a transação for cancelada	Gravar			
DeregisterResource	Concede permissão para cancelar o registro de um local registrado	Gravar			
DescribeLakeFormationIdentityCenterConfiguration	Concede permissão para descrever a conexão do Centro de Identidade do IAM com o Lake Formation	Leitura			
DescribeResource	Concede permissão para descrever um local registrado	Leitura			
DescribeTransaction	Concede permissão para obter o status da transação específica	Leitura			
ExtendTransaction	Concede permissão para estender o tempo limite da transação específica	Gravar			
GetDataAccess	Concede permissão para acessar o data lake virtual	Gravar		lakeformation:EnabledOnlyForMetaDataAccess	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetDataCellsFilter	Concede permissão para recuperar um filtro de célula de dados do Lake Formation	Leitura			
GetDataLakePrincipal	Concede permissão para recuperar a identidade da entidade principal invocadora	Leitura			
GetDataLakeSettings	Concede permissão para recuperar as configurações de data lake, como a lista de administradores de data lake e permissões padrão de banco de dados e tabela	Leitura			
GetEffectivePermissionsForPath	Concede permissão para recuperar permissões anexadas a recursos no caminho especificado	Leitura			
GetLFTag	Concede permissão para recuperar uma etiqueta do Lake Formation	Leitura			
GetLFTagExpression	Concede permissão para recuperar uma expressão de tag do Lake Formation	Leitura			
GetQueryState	Concede permissão para recuperar o estado da consulta específica	Leitura			lakeformation:StartQueryPlanning

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetQueryStatistics	Concede permissão para recuperar a estatística da consulta específica	Leitura			lakeformation:StartQueryPlanning
GetResourceLFTags	Concede permissão para recuperar etiquetas de lakeformation em um recurso do catálogo	Leitura			
GetTableObjects	Concede permissão para recuperar objetos de uma tabela	Leitura			
GetWorkUnitResults	Concede permissão para recuperar os resultados das unidades de trabalho específicas	Leitura			lakeformation:GetWorkUnits lakeformation:StartQueryPlanning
GetWorkUnits	Concede permissão para recuperar as unidades de trabalho da consulta específica	Leitura			lakeformation:StartQueryPlanning
GrantPermissions	Concede permissão para permissões de data lake a um principal	Gerenciamento de permissões			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDataCellsFilter	Concede permissão para listar filtros de célula	Lista			
ListLFTagExpressions	Concede permissão para listar expressões de tag do Lake Formation	Leitura			
ListLFTags	Concede permissão para listar etiquetas do Lake Formation	Leitura			
ListLakeFormationOptIns	Concede permissão para recuperar a lista atual de recursos e entidades principais que optaram por impor permissões do Lake Formation	Lista			
ListPermissions	Concede permissão para listar as permissões filtradas pelo primário ou pelo recurso	Lista			
ListResources	Concede permissão para listar locais registrados	Lista			
ListTableStorageOptimizers	Concede permissão para listar todos os otimizadores de armazenamento da tabela Governed	Lista			
ListTransactions	Concede permissão para listar todas as transações no sistema	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutDataLakeSettings	Concede permissão para substituir as configurações de data lake, como a lista de administradores de data lake e permissões padrão de banco de dados e tabela	Gerenciamento de permissões			
RegisterResource	Concede permissão para registrar um novo local a ser gerenciado por Lake Formation	Gravar			
RegisterResourceWithPrivilegedAccess	Concede permissão para registrar um novo local a ser administrado pela Lake Formation, com acesso privilegiado	Gravar			
RemoveLFTagsFromResource	Concede permissão para remover etiquetas de lakeformation de recursos do catálogo	Tags			
RevokePermissions	Concede permissão para revogar permissões de data lake de um primário	Gerenciamento de permissões			
SearchDatabasesByLFTags	Concede permissão para listar bancos de dados de catálogos com etiquetas do Lake Formation	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SearchTablesByLFTags	Concede permissão para listar tabelas de catálogos com etiquetas do Lake Formation	Leitura			
StartQueryPlanning	Concede permissão para iniciar o planejamento da consulta específica	Gravar			
StartTransaction	Concede permissão para iniciar uma nova transação	Gravar			
UpdateDataCellsFilter	Concede permissão para atualizar um filtro de célula de dados do Lake Formation	Gravar			
UpdateLFTag	Concede permissão para atualizar uma etiqueta do Lake Formation	Gravar			
UpdateLFTagExpression	Concede permissão para atualizar uma expressão de Lake Formation	Gravar			
UpdateLakeFormationIdentityCenterConfiguration	Concede permissão para atualizar os parâmetros de conexão do Centro de Identidade do IAM	Gravar			
UpdateResource	Concede permissão para atualizar um local registrado	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateTableObjects	Concede permissão para adicionar os objetos especificados a uma tabela ou excluí-los	Gravar			
UpdateTableStorageOptimizer	Concede permissão para atualizar a configuração do otimizador de armazenamento para a tabela Governed	Gravar			

Tipos de recursos definidos pelo AWS Lake Formation

AWS O Lake Formation não suporta a especificação de um ARN de recurso no elemento de uma `Resource` declaração de política do IAM. Para permitir acesso ao AWS Lake Formation, especifique `"Resource": "*"` na política.

Chaves de condição do AWS Lake Formation

AWS O Lake Formation define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
lakeformation:EnabledOnlyFo	Filtra o acesso pela presença da chave configurada para a política baseada em identidade da função	Bool

Chaves de condição	Descrição	Tipo
rMetaData Access		

Ações, recursos e chaves de condição do AWS Lambda

AWS O Lambda (prefixo do serviço:`lambda`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Lambda
- Tipos de recursos definidos pelo AWS Lambda
- Chaves de condição do AWS Lambda

Ações definidas pelo AWS Lambda

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddLayerVersionPermission	Concede permissão para adicionar permissões à política baseada em recursos de uma versão de uma camada AWS Lambda	Gerenciamento de permissões	layerVersion*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddPermission	Concede permissão para dar permissão a um AWS serviço ou outra conta para usar uma função AWS Lambda	Gerenciamento de permissões	function*		
				lambda:Principal lambda:FunctionUrlAuthType	
CreateAlias	Concede permissão para criar um alias para uma versão de função do Lambda	Gravar	function*		
CreateCodeSigningConfig	Concede permissão para criar uma configuração de AWS assinatura de código Lambda	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventSourceMapping	Concede permissão para criar um mapeamento entre uma fonte de eventos e uma função AWS Lambda	Gravar		lambda:FunctionArn aws:RequestTag/${TagKey} aws:TagKeys	
CreateFunction	Concede permissão para criar uma função AWS Lambda	Gravar	function*		iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				lambda:Layer lambda:VpcIds lambda:SubnetIds lambda:SecurityGroupIds lambda:CodeSigningConfigArn aws:RequestTag/${TagKey} aws:TagKeys	
CreateFunctionUrlConfig	Concede permissão para criar uma configuração de URL de função para uma função Lambda	Gravar	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteAlias	Concede permissão para excluir um alias da AWS função Lambda	Gravar	function*		
DeleteCodeSigningConfig	Concede permissão para excluir uma configuração de AWS assinatura de código Lambda	Gravar	codesigningconfig*		
DeleteEventSourceMapping	Concede permissão para excluir um mapeamento de AWS origem de eventos do Lambda	Gravar	eventSourceMapping*		
				lambda:FunctionArn	
DeleteFunction	Concede permissão para excluir uma função AWS Lambda	Gravar	function*		
DeleteFunctionCodeSigningConfig	Concede permissão para separar uma configuração de assinatura de código de uma função AWS Lambda	Gravar	function*		
DeleteFunctionConcurrency	Concede permissão para remover um limite de execução simultânea de uma função AWS Lambda	Gravar	function*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteFunctionEventInvokeConfig	Concede permissão para excluir a configuração para invocação assíncrona para uma função, versão ou alias do AWS Lambda	Gravar	function*		
DeleteFunctionUrlConfig	Concede permissão para excluir uma configuração de URL de função para uma função Lambda	Gravar	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	
DeleteLayerVersion	Concede permissão para excluir uma versão de uma camada AWS Lambda	Gravar	layerVersion*		
DeleteProvisionedConcurrencyConfig	Concede permissão para excluir a configuração de simultaneidade provisionada para uma função Lambda AWS	Gravar	function alias		
			function version		
DisableReplication [somente permissão]	Concede permissão para desativar a replicação para uma função do Lambda@Edge	Permissions management	function*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
EnableReplication [somente permissão]	Concede permissão para habilitar a replicação para uma função do Lambda@Edge	Gerenciamento de permissões	function*		
GetAccountSettings	Concede permissão para visualizar detalhes sobre os limites e o uso de uma conta em um Região da AWS	Leitura			
GetAlias	Concede permissão para visualizar detalhes sobre um alias de AWS função Lambda	Leitura	function*		
GetCodeSigningConfig	Concede permissão para visualizar detalhes sobre uma configuração de AWS assinatura de código Lambda	Leitura	code signing config*		
GetEventSourceMapping	Concede permissão para visualizar detalhes sobre o mapeamento da fonte de um evento AWS Lambda	Leitura	eventSourceMapping*		
				lambda:FunctionArn	
GetFunction	Concede permissão para visualizar detalhes sobre uma função AWS Lambda	Leitura	function*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetFunctionCodeSigningConfig	Concede permissão para visualizar o arn de configuração de assinatura de código anexado a uma função AWS Lambda	Leitura	function*		
GetFunctionConcurrency	Concede permissão para exibir detalhes sobre a configuração de simultaneidade reservada para uma função	Leitura	function*		
GetFunctionConfiguration	Concede permissão para visualizar detalhes sobre as configurações específicas da versão de uma função ou versão do AWS Lambda	Leitura	function*		
GetFunctionEventInvokeConfig	Concede permissão para exibir a configuração para invocação assíncrona de uma função, uma versão ou um alias	Leitura	function*		
GetFunctionRecursionConfig	Concede permissão para visualizar a configuração de recursão de uma função AWS Lambda	Leitura	function*		
GetFunctionUrlConfig	Concede permissão para ler uma configuração de URL de função para uma função Lambda	Leitura	function*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				lambda:FunctionUrlAuthType lambda:FunctionArn	
GetLayerVersion	Concede permissão para visualizar detalhes sobre uma versão de uma camada AWS Lambda. Observe que essa ação também oferece suporte à GetLayerVersionByArn API.	Leitura	layerVersion*		
GetLayerVersionPolicy	Concede permissão para visualizar a política baseada em recursos para uma versão de uma camada AWS Lambda	Leitura	layerVersion*		
GetPolicy	Concede permissão para visualizar a política baseada em recursos para uma função, versão ou alias do AWS Lambda	Leitura	function*		
GetProvisionedConcurrencyConfig	Concede permissão para visualizar a configuração de simultaneidade provisionada para o alias ou a versão de uma função AWS Lambda	Leitura	function alias		
			function version		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetRuntimeManagementConfig	Concede permissão para visualizar a configuração de gerenciamento de tempo de execução de uma função AWS Lambda	Leitura	function*		
InvokeAsync	Concede permissão para invocar uma função de forma assíncrona (Defasado)	Gravar	function*		
InvokeFunction	Concede permissão para invocar uma função AWS Lambda	Gravar	function*		
				lambda:EventSourceToken	
InvokeFunctionUrl [somente permissão]	Concede permissão para invocar uma função AWS Lambda por meio de url	Gravar	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn lambda:EventSourceToken	
ListAliases	Concede permissão para recuperar uma lista de aliases para uma função AWS Lambda	Lista	function*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListCodeSigningConfigs	Concede permissão para recuperar uma lista de configurações de assinatura de AWS código Lambda	Lista			
ListEventSourceMappings	Concede permissão para recuperar uma lista de mapeamentos de origem de AWS eventos do Lambda	Lista			
ListFunctionEventInvokeConfigs	Concede permissão para recuperar uma lista de configurações para invocação assíncrona de uma função	Lista	function*		
ListFunctionUrlConfigs	Concede permissão para ler configurações de URL de função para uma função	Lista	function*		
				lambda:FunctionUrlAuthType	
ListFunctions	Concede permissão para recuperar uma lista de funções do AWS Lambda, com a configuração específica da versão de cada função	Lista			
ListFunctionsByCodeSigningConfig	Concede permissão para recuperar uma lista de funções do AWS Lambda pela configuração de assinatura de código atribuída	Lista	code signing config*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListLayerVersions	Concede permissão para recuperar uma lista de versões de uma camada AWS Lambda	Lista			
ListLayers	Concede permissão para recuperar uma lista de camadas do AWS Lambda, com detalhes sobre a versão mais recente de cada camada	Lista			
ListProvisionedConcurrencyConfigs	Concede permissão para recuperar uma lista de configurações de simultaneidade provisionadas para uma função Lambda AWS	Lista	function*		
ListTags	Concede permissão para recuperar uma lista de tags para uma função AWS Lambda, mapeamento da fonte de eventos ou recurso de configuração de assinatura de código	Leitura	code signing config		
			eventSourceMapping		
			function		
ListVersionsByFunction	Concede permissão para recuperar uma lista de versões de uma função AWS Lambda	Lista	function*		
PublishLayerVersion	Concede permissão para criar uma camada AWS Lambda	Gravar	layer*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PublishVersion	Concede permissão para criar uma versão da AWS função Lambda	Gravar	function*		
PutFunctionCodeSigningConfig	Concede permissão para anexar uma configuração de assinatura de código a uma função AWS Lambda	Gravar	code signing config*		
			function*		
				lambda:CodeSigningConfigArn	
PutFunctionConcurrency	Concede permissão para configurar a simultaneidade reservada para uma função AWS Lambda	Gravar	function*		
PutFunctionEventInvokeConfig	Concede permissão para configurar opções para invocação assíncrona em uma função, versão ou alias do AWS Lambda	Gravar	function*		
PutFunctionRecursionConfig	Concede permissão para atualizar a configuração de recursão de uma função AWS Lambda	Gravar	function*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutProvisionedConcurrencyConfig	Concede permissão para configurar a simultaneidade provisionada para o alias ou a versão de uma função AWS Lambda	Gravar	function alias		
			function version		
PutRuntimeManagementConfig	Concede permissão para atualizar a configuração de gerenciamento de tempo de execução de uma função AWS Lambda	Gravar	function*		
RemoveLayerVersionPermission	Concede permissão para remover uma declaração da política de permissões para uma versão de uma camada AWS Lambda	Gerenciamento de permissões	layerVersion*		
RemovePermission	Concede permissão para revogar a permissão de uso de funções de um AWS serviço ou de outra conta	Gerenciamento de permissões	function*		
				lambda:Principal lambda:FunctionUrlAuthType	
TagResource	Concede permissão para adicionar tags a uma função AWS Lambda, mapeamento da fonte de eventos ou recurso de configuração de assinatura de código	Tags	code signing config		
			eventSourceMapping		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			function		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover tags de uma função AWS Lambda, mapeamento da fonte de eventos ou recurso de configuração de assinatura de código	Tags	code signing config		
			eventSourceMapping		
			function		
				aws:TagKeys	
UpdateAlias	Concede permissão para atualizar a configuração do alias de uma função AWS Lambda	Gravar	function*		
UpdateCodeSigningConfig	Concede permissão para atualizar uma configuração de AWS assinatura de código Lambda	Gravar	code signing config*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateEventSourceMapping	Concede permissão para atualizar a configuração de um mapeamento de origem de eventos AWS Lambda	Gravar	eventSourceMapping*		
				lambda:FunctionArn	
UpdateFunctionCode	Concede permissão para atualizar o código de uma função AWS Lambda	Gravar	function*		
UpdateFunctionCodeSigningConfig	Concede permissão para atualizar a configuração de assinatura de código de uma função AWS Lambda	Gravar	codesigningconfig*		
			function*		
UpdateFunctionConfiguration	Concede permissão para modificar as configurações específicas da versão de uma função AWS Lambda	Gravar	function*		
				lambda:Layer lambda:VpcIds lambda:SubnetIds lambda:SecurityGroupIds	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateFunctionEventInvokeConfig	Concede permissão para modificar a configuração para invocação assíncrona para uma função, versão ou alias do AWS Lambda	Gravar	function*		
UpdateFunctionUrlConfig	Concede permissão para atualizar uma configuração de URL de função para uma função Lambda	Gravar	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	

Tipos de recursos definidos pelo AWS Lambda

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
code signing config	`arn:${Partition}:lambda:${Region}:${Account}:code-signing-config:${CodeSigningConfigId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
eventSourceMapping	`arn:${Partition}:lambda:${Region}:${Account}:event-source-mapping:${UUID}`	aws:ResourceTag/${TagKey}
function	`arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}`	aws:ResourceTag/${TagKey}
function alias	`arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}:${Alias}`	aws:ResourceTag/${TagKey}
function version	`arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}:${Version}`	aws:ResourceTag/${TagKey}
layer	`arn:${Partition}:lambda:${Region}:${Account}:layer:${LayerName}`	
layerVersion	`arn:${Partition}:lambda:${Region}:${Account}:layer:${LayerName}:${LayerVersion}`	

Chaves de condição do AWS Lambda

AWS O Lambda define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString
lambda:CodeSigningConfigArn	Filtra o acesso pelo ARN de uma configuração de assinatura de código AWS Lambda	ARN
lambda:EventSourceToken	Filtra o acesso pelo ID de uma fonte sem AWS eventos configurada para a função AWS Lambda	String
lambda:FunctionArn	Filtra o acesso pelo ARN de uma função AWS Lambda	ARN
lambda:FunctionUrlAuthType	Filtra o acesso por tipo de autorização especificado na solicitação. Disponível durante CreateFunctionUrlConfig, UpdateFunctionUrlConfig DeleteFunctionUrlConfig, GetFunctionUrlConfig, ListFunctionUrlConfig, AddPermission e RemovePermission operações	String
lambda:Layer	Filtra o acesso pelo ARN de uma versão de uma camada AWS Lambda	ArrayOfString
lambda:Principal	Filtra o acesso restringindo o AWS serviço ou a conta que pode invocar uma função	String
lambda:SecurityGroupIds	Filtra o acesso pelo ID dos grupos de segurança configurados para a função AWS Lambda	ArrayOfString

Chaves de condição	Descrição	Tipo
lambda:SourceFunctionArn	Filtra o acesso pelo ARN da função Lambda da qual a AWS solicitação foi originada	ARN
lambda:SubnetIds	Filtra o acesso pelo ID das sub-redes configuradas para a função AWS Lambda	ArrayOfString
lambda:VpcIds	Filtra o acesso pelo ID da VPC configurada para a função AWS Lambda	String

Ações, recursos e chaves de condição para o AWS Launch Wizard

AWS O Launch Wizard (prefixo do serviço:`launchwizard`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Launch Wizard
- Tipos de recursos definidos pelo AWS Launch Wizard
- Chaves de condição para o AWS Launch Wizard

Ações definidas pelo AWS Launch Wizard

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAdditionalNode [somente permissão]	Concede permissão para criar um nó adicional	Gravar			
CreateDeployment	Concede permissão para criar uma implantação	Gravar	deployment*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateSettingsSet [somente permissão]	Concede permissão para criar um conjunto de configurações de aplicativo	Gravar			
DeleteAdditionalNode [somente permissão]	Concede permissão para excluir um nó adicional	Gravar			
DeleteApp [somente permissão]	Concede permissão para excluir um aplicativo	Gravar			
DeleteDeployment	Concede permissão para excluir uma implantação	Gravar	deployment*	aws:ResourceTag/${TagKey}	
DeleteSettingsSet	Concede permissão para excluir configurações definidas	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
[somente permissão]					
DescribeAdditionalNode [somente permissão]	Concede permissão para descrever um nó adicional	Leitura			
DescribeProvisionedApp [somente permissão]	Concede permissão para descrever aplicações de provisionamento	Leitura			
DescribeProvisioningEvents [somente permissão]	Concede permissão para descrever eventos de provisionamento	Leitura			
DescribeSettingsSet [somente permissão]	Concede permissão para descrever um conjunto de configurações de aplicativo	Leitura			
GetDeployment	Concede permissão para obter uma implantação	Leitura	deployment*	aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetInfrastructureSuggestion [somente permissão]	Concede permissão para obter sugestão de infraestrutura	Leitura			
GetIpAddress [somente permissão]	Concede permissão para obter o endereço IP do cliente	Leitura			
GetResourceCostEstimate [somente permissão]	Concede permissão para obter estimativas de custo de recurso	Leitura			
GetResourceRecommendation [somente permissão]	Concede permissão para obter recomendações para um recurso	Leitura			
GetSettingsSet [somente permissão]	Concede permissão para obter configurações definidas	Leitura			
GetWorkload	Concede permissão para obter uma workload	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetWorkloadAsset [somente permissão]	Concede permissão para obter um ativo da workload	Leitura			
GetWorkloadAssets [somente permissão]	Concede permissão para obter ativos de workload	Leitura			
GetWorkloadDeploymentPattern	Concede permissão para obter um padrão de implantação	Leitura			
ListAdditionalNodes [somente permissão]	Concede permissão para listar nós adicionais	Lista			
ListAllowedResources [somente permissão]	Concede permissão para listar os recursos permitidos	Lista			
ListDeploymentEvents	Concede permissão para listar os eventos que ocorreram durante uma implantação	Lista			
ListDeployments	Concede permissão para listar implantações	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListProvisionedApps [somente permissão]	Concede permissão para listar aplicações de provisionamento	Lista			
ListResourceCostEstimates [somente permissão]	Concede permissão para listar estimativas de custos de recursos	Lista			
ListSettingsSets [somente permissão]	Concede permissão para listar configurações definidas	Lista			
ListTagsForResource	Concede permissão para listar tags para um LaunchWizard recurso.	Leitura	deployment	aws:ResourceTag/${TagKey}	
ListWorkloadDeploymentOptions [somente permissão]	Concede permissão para listar as opções de implantação de uma determinada workload	Lista			
ListWorkloadDeploymentPatterns	Concede permissão para listar os padrões de implantação de uma workload	Lista			
ListWorkloads	Concede permissão para listar cargas de trabalho	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutSettingsSet [somente permissão]	Concede permissão para criar configurações definidas	Gravar			
StartProvisioning [somente permissão]	Concede permissão para iniciar um provisionamento	Gravar			
TagResource	Concede permissão para marcar um LaunchWizard recurso.	Tags	deployment	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permissão para desmarcar um LaunchWizard recurso.	Tags	deployment	aws:TagKeys	
UpdateSettingsSet [somente permissão]	Concede permissão para atualizar um conjunto de configurações de aplicativo	Gravar			

Tipos de recursos definidos pelo AWS Launch Wizard

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
deployment	`arn:${Partition}:launchwizard:${Region}:${Account}:deployment/${DeploymentId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o AWS Launch Wizard

AWS O Launch Wizard define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso com base na presença de pares de chave/valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso com base nos pares de chave-valor da etiqueta anexados ao recurso	String

Chaves de condição	Descrição	Type
aws:TagKeys	Filtra o acesso com base na presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Lex

O Amazon Lex (prefixo do serviço: `lex`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Lex
- Tipos de recursos definidos pelo Amazon Lex
- Chaves de condição do Amazon Lex

Ações definidas pelo Amazon Lex

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateBotVersion	Cria uma nova versão com base na versão $LATEST do bot especificado	Gravar	bot version*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateIntentVersion	Cria uma nova versão com base na versão $LATEST da intenção especificada	Gravar	intent version*		
CreateSlotTypeVersion	Cria uma nova versão com base na versão $LATEST do tipo de slot especificado	Gravar	slottype version*		
DeleteBot	Exclui todas as versões de um bot	Gravar	bot version*		
DeleteBotAlias	Exclui um alias de um bot específico	Gravar	bot alias*		
DeleteBotChannelAssociation	Exclui a associação entre um alias de bot do Amazon Lex e uma plataforma de sistema de mensagens	Gravar	channel*		
DeleteBotVersion	Exclui uma versão específica de um bot	Gravar	bot version*		
DeleteIntent	Exclui todas as versões de uma intenção	Gravar	intent version*		
DeleteIntentVersion	Exclui uma versão específica de uma intenção	Gravar	intent version*		
DeleteSession	Remove informações de sessão para um bot, alias e ID de usuário especificado	Gravar	bot alias		
			bot version		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteSlotType	Exclui todas as versões de um tipo de slot	Gravar	slottype version*		
DeleteSlotTypeVersion	Exclui uma versão específica de um tipo de slot	Gravar	slottype version*		
DeleteUtterances	Exclui as informações que o Amazon Lex mantém para enunciados em um bot e userId específicos	Gravar	bot version*		
GetBot	Retorna informações para um bot específico. Além do nome do bot, a versão ou o alias do bot é necessário	Leitura	bot alias		
			bot version		
GetBotAlias	Retorna informações sobre um alias de bot do Amazon Lex	Leitura	bot alias*		
GetBotAliases	Retorna uma lista de alias para determinado bot do Amazon Lex	Lista			
GetBotChannelAssociation	Retorna informações sobre a associação entre um bot do Amazon Lex e uma plataforma de sistema de mensagens	Leitura	channel*		
GetBotChannelAssociations	Retorna uma lista de todos os canais associados a um único bot	Lista	channel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetBotVersions	Retorna informações sobre todas as versões de um bot específico	Lista	bot version*		
GetBots	Retorna informações sobre a versão $LATEST de todos os bots, sujeitas a filtros fornecidos pelo cliente	Lista			
GetBuiltinIntent	Retorna informações sobre uma intenção integrada	Leitura			
GetBuiltinIntents	Obtém uma lista de intenções integradas que atendem aos critérios especificados	Leitura			
GetBuiltinSlotTypes	Obtém uma lista dos tipos de slots integrados que atendem aos critérios especificados	Leitura			
GetExport	Exporta o recurso do Amazon Lex em um formato solicitado	Leitura	bot version*		
GetImport	Obtém informações sobre um trabalho de importação iniciado com StartImport	Leitura			
GetIntent	Retorna informações sobre uma intenção específica. Além do nome da intenção, também é necessário especificar a versão da intenção	Leitura	intent version*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetIntentVersions	Retorna informações sobre todas as versões de uma intenção específica	Lista	intent version*		
GetIntents	Retorna informações sobre a versão $LATEST de todas as intenções, sujeitas a filtros fornecidos pelo cliente	Lista			
GetMigration	Concede permissão para visualizar uma migração em andamento ou concluída	Leitura			
GetMigrations	Concede permissão para visualizar a lista de migrações do Amazon Lex v1 para o Amazon Lex v2	Lista			
GetSession	Retorna informações de sessão para um bot, alias e ID de usuário especificado	Leitura	bot alias		
			bot version		
GetSlotType	Retorna informações sobre uma versão específica de um tipo de slot. Além de especificar o nome do tipo de slot, também é necessário especificar a versão do tipo de slot	Leitura	slottype version*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSlotTypeVersions	Retorna informações sobre todas as versões de um tipo de slot específico	Lista	slottype version*		
GetSlotTypes	Retorna informações sobre a versão $LATEST de todos os tipos de slots, sujeitas a filtros fornecidos pelo cliente	Lista			
GetUtterancesView	Retorna uma visualização dos dados dos enunciados agregados das versões de um bot para um período recente	Lista	bot version*		
ListTagsForResource	Lista etiquetas para um recurso do Lex	Leitura	bot		
			bot alias		
			channel		
PostContent	Envia a entrada do usuário (texto ou fala) ao Amazon Lex	Gravar	bot alias		
			bot version		
PostText	Envia a entrada do usuário (somente texto) ao Amazon Lex	Gravar	bot alias		
			bot version		
PutBot	Cria ou atualiza a versão $LATEST de um bot de conversação do Amazon Lex	Gravar	bot version*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
PutBotAlias	Cria ou atualiza um alias para o bot específico	Gravar	bot alias*		
				aws:TagKeys aws:RequestTag/${TagKey}	
PutIntent	Cria ou atualiza a versão $LATEST de uma intenção	Gravar	intent version*		
PutSession	Cria uma nova sessão ou modifica uma sessão existente com um bot do Amazon Lex	Gravar	bot alias		
			bot version		
PutSlotType	Cria ou atualiza a versão $LATEST de um tipo de slot	Gravar	slottype version*		
StartImport	Inicia um trabalho para importar um recurso para o Amazon Lex	Gravar			
StartMigration	Concede permissão para migrar um bot do Amazon Lex v1 para o Amazon Lex v2	Gravar	bot version*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Adiciona ou substitui etiquetas a um recurso do Lex	Marcação	bot		
			bot alias		
			channel		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Remove etiquetas de um recurso do Lex	Marcação	bot		
			bot alias		
			channel		
				aws:TagKeys aws:RequestTag/${TagKey}	

Tipos de recursos definidos pelo Amazon Lex

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}`	

Chaves de condição do Amazon Lex

O Amazon Lex define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso com base nas tags da solicitação.	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas anexadas a um recurso do Lex.	String
aws:TagKeys	Filtra o acesso com base no conjunto de chaves da etiqueta na solicitação	ArrayOfString
lex:associatedIntents	Permite que você controle o acesso com base nas intenções incluídas na solicitação	ArrayOfString
lex:associatedSlotTypes	Permite que você controle o acesso com base nos tipos de slot incluídos na solicitação	ArrayOfString
lex:channelType	Permite que você controle o acesso com base no tipo de canal incluído na solicitação	String

Ações, recursos e chaves de condição do Amazon Lex V2

O Amazon Lex V2 (prefixo do serviço: `lex`) fornece os recursos, ações e chaves de contexto de condição a seguir, específicos do serviço, para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Lex V2
- Tipos de recursos definidos pelo Amazon Lex V2
- Chaves de condição do Amazon Lex V2

Ações definidas pelo Amazon Lex V2

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchCreateCustomVocabularyItem	Concede permissão para criar novos itens em um vocabulário personalizado existente	Gravar	bot*		
BatchDeleteCustomVocabularyItem	Concede permissão para excluir itens existentes em um vocabulário personalizado existente	Gravar	bot*		
BatchUpdateCustomVocabularyItem	Concede permissão para atualizar itens existentes em um vocabulário personalizado existente	Gravar	bot*		
BuildBotLocale	Concede permissão para criar um local de bot existente em um bot	Gravação	bot*		
CreateBot	Concede permissão para criar um novo bot e um alias de bot de teste apontando para a versão de RASCUNHO do bot	Gravação	bot*		
			bot alias*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateBotAlias		Gravação	bot alias*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	Concede permissão para criar um novo alias de bot em um bot			aws:TagKeys aws:RequestTag/${TagKey}	
CreateBotChannel [somente permissão]	Concede permissão para criar um canal de bot em um bot existente	Gravação	bot*		
CreateBotLocale	Concede permissão para criar um novo local de bot em um bot existente	Gravar	bot*		
CreateBotReplica	Concede permissão para criar uma réplica de bot para um bot	Gravar	bot*		
CreateBotVersion	Concede permissão para criar uma nova versão de um bot existente	Gravar	bot*		
CreateCustomVocabulary [somente permissão]	Concede permissão para criar um novo vocabulário personalizado em um local de bot existente	Gravar	bot*		
CreateExport	Concede permissão para criar uma exportação para um recurso existente	Gravação	bot test set		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateIntent	Concede permissão para criar uma nova intenção em um local de bot existente	Gravação	bot*		
CreateResourcePolicy	Concede permissão para criar uma nova política de recursos para um recurso do Lex	Gravar	bot		
			bot alias		
CreateResourcePolicyStatement	Concede permissão para criar uma nova declaração de política de recursos para um recurso do Lex	Gravar	bot		
			bot alias		
CreateSlot	Concede permissão para criar um novo slot em uma intenção	Gravação	bot*		
CreateSlotType	Concede permissão para criar um novo tipo de slot em um local de bot existente	Gravar	bot*		
CreateTestSet [somente permissão]	Concede permissão para importar num novo conjunto de testes	Gravar			
CreateTestSetDiscrepancyReport	Concede permissão para criar um relatório de discrepância de conjunto de testes	Gravar	test set*		
CreateUploadUrl	Concede permissão para criar um URL de upload para arquivo de importação	Gravação			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteBot	Concede permissão para excluir um bot existente	Gravação	bot*		lex:DeleteBotAlias lex:DeleteBotChannel lex:DeleteBotLocale lex:DeleteBotVersion lex:DeleteIntent lex:DeleteSlot lex:DeleteSlotType
			bot alias*		
DeleteBotAlias	Concede permissão para excluir um alias de bot existente em um bot	Gravação	bot alias*		
DeleteBotChannel [somente permissão]	Concede permissão para excluir um canal de bot existente	Gravação	bot*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteBotLocale	Concede permissão para excluir um local de bot existente em um bot	Gravar	bot*		lex:DeleteIntent lex:DeleteSlot lex:DeleteSlotType
DeleteBotReplica	Concede permissão para excluir uma réplica de bot existente	Gravar	bot*		
DeleteBotVersion	Concede permissão para excluir uma versão do bot existente	Gravar	bot*		
DeleteCustomVocabulary	Concede permissão para excluir um vocabulário personalizado existente em um local de bot	Gravar	bot*		
DeleteExport	Concede permissão para excluir uma exportação existente	Gravação	bot		
			test set		
DeleteImport	Concede permissão para excluir uma importação existente	Gravação	bot		
			test set		
DeleteIntent	Concede permissão para excluir uma intenção existente em um local de bot	Gravação	bot*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteResourcePolicy	Concede permissão para excluir uma política de recursos existente para um recurso do Lex	Gravar	bot		
			bot alias		
DeleteResourcePolicyStatement	Concede permissão para excluir uma declaração de política de recursos existente para um recurso do Lex	Gravar	bot		
			bot alias		
DeleteSession	Concede permissão para excluir as informações da sessão para um alias de bot e o ID do usuário	Gravação	bot alias*		
DeleteSlot	Concede permissão para excluir um slot existente em uma intenção	Gravação	bot*		
DeleteSlotType	Concede permissão para excluir um tipo de slot existente em um local de bot	Gravar	bot*		
DeleteTestSet	Concede permissão para excluir um conjunto de testes existente	Gravar	test set*		
DeleteUtterances	Concede permissão para excluir dados de enunciados de um bot	Gravar	bot*		
DescribeBot	Concede permissão para recuperar um bot existente	Leitura	bot*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeBotAlias	Concede permissão para recuperar um alias de bot existente	Leitura	bot alias*		
DescribeBotChannel [somente permissão]	Concede permissão para recuperar um canal de bot existente	Leitura	bot*		
DescribeBotLocale	Concede permissão para recuperar um local de bot existente	Leitura	bot*		
DescribeBotRecommendation	Concede permissão para recuperar informações de metadados sobre uma recomendação de bot	Leitura	bot*		
DescribeBotReplica	Concede permissão para recuperar uma réplica de bot existente	Leitura	bot*		
DescribeBotResourceGeneration	Concede permissão para recuperar informações de metadados para uma geração de recurso de bot	Leitura	bot*		
DescribeBotVersion	Concede permissão para recuperar uma versão de bot existente	Leitura	bot*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeCustomVocabulary [somente permissão]	Concede permissão para recuperar um vocabulário personalizado existente	Leitura	bot*		
DescribeCustomVocabularyMetadata	Concede permissão para recuperar metadados de um vocabulário personalizado existente	Leitura	bot*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeExport	Concede permissão para recuperar uma exportação existente	Leitura	bot		lex:DescribeBot lex:DescribeBotLocale lex:DescribeIntent lex:DescribeSlot lex:DescribeSlotType lex:ListBotLocales lex:ListIntents lex:ListSlotTypes lex:ListSlots
			test set		
DescribeImport	Concede permissão para recuperar uma importação existente	Leitura	bot		
			test set		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeIntent	Concede permissão para recuperar uma intenção existente	Leitura	bot*		
DescribeResourcePolicy	Concede permissão para recuperar uma política de recursos existente para um recurso do Lex	Leitura	bot		
			bot alias		
DescribeSlot	Concede permissão para recuperar um slot existente	Leitura	bot*		
DescribeSlotType	Concede permissão para recuperar um tipo de slot existente	Leitura	bot*		
DescribeTestExecution	Concede permissão para recuperar metadados de execução de teste	Leitura	test set*		
DescribeTestSet	Concede permissão para recuperar um conjunto de testes existente	Leitura	test set*		
DescribeTestSetDiscrepancyReport	Concede permissão para recuperar metadados de relatório de discrepância de conjunto de testes	Leitura	test set*		
DescribeTestSetGeneration	Concede permissão para recuperar metadados de geração de conjunto de testes	Leitura	test set		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GenerateBotElement	Concede permissão para gerar campos ou elementos compatíveis para um bot	Leitura	bot*		
GetSession	Concede permissão para recuperar informações da sessão para um alias de bot e o ID de usuário	Leitura	bot alias*		
GetTestExecutionArtifactsUrl	Concede permissão para recuperar o URL de artefatos para uma execução de teste	Leitura	test set*		
ListAggregatedUtterances	Concede permissão para listar enunciados e estatísticas de um bot	Lista	bot*		
ListBotAliasReplicas	Concede permissão para listar réplicas de alias em uma réplica de bot	Lista	bot*		
ListBotAliases	Concede permissão para listar os aliases de bot em um bot	List	bot*		
ListBotChannels [somente permissão]	Concede permissão para listar os canais de bot	List	bot*		
ListBotLocales	Concede permissão para listar os locais de bot em um bot	Lista	bot*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListBotRecommendations	Concede permissão para obter uma lista de recomendações de bot que atendem aos critérios especificados	Lista	bot*		
ListBotReplicas	Concede permissão para listar réplicas de um bot	Lista	bot*		
ListBotResourceGenerations	Concede permissão para listar as gerações de recurso para um bot	Lista	bot*		
ListBotVersionReplicas	Concede permissão para listar réplicas de versão em uma réplica de bot	Lista	bot*		
ListBotVersions	Concede permissão para listar versões de bot existentes	List	bot*		
ListBots	Concede permissão para listar bots existentes	List			
ListBuiltInIntents	Concede permissão para listar as intenções integradas	List			
ListBuiltInSlotTypes	Concede permissão para listar os tipos de slot integrados	Lista			
ListCustomVocabularyItems	Concede permissão para listar itens de um vocabulário personalizado existente	Lista	bot*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListExports	Concede permissão para relacionar exportações existentes	List			
ListImports	Concede permissão para relacionar importações existentes	Lista			
ListIntentMetrics	Concede permissão para listar métricas de analytics de intenção para um bot	Lista	bot*		
ListIntentPaths	Concede permissão para listar o analytics de caminhos de intenção para um bot	Lista	bot*		
ListIntentStageMetrics	Concede permissão para listar métricas de analytics do IntentStage para um bot	Lista	bot*		
ListIntents	Concede permissão para listar intenções em um bot	Lista	bot*		
ListRecommendedIntents	Concede permissão para obter uma lista de intenções recomendadas fornecidas pela recomendação de bot	Lista	bot*		
ListSessionAnalyticsData	Concede permissão para listar dados de analytics de sessão para um bot	Lista	bot*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListSessionMetrics	Concede permissão para listar métricas de analytics de sessão para um bot	Lista	bot*		
ListSlotTypes	Concede permissão para listar os tipos de slot em um bot	List	bot*		
ListSlots	Concede permissão para listar slots em uma intenção	List	bot*		
ListTagsForResource	Concede permissão para listar as etiquetas para um recurso Lex	Leitura	bot		
			bot alias		
			test set		
ListTestExecutionResultItems	Concede permissão para recuperar dados de resultados de teste para uma execução de teste	Leitura	test set*		lex:ListTestSetRecords
ListTestExecutions	Concede permissão para listar execuções de teste	Lista			
ListTestSetRecords	Concede permissão para recuperar registros dentro de um conjunto de testes existente	Leitura	test set*		
ListTestSets	Concede permissão para listar conjuntos de testes	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutSession	Concede permissão para criar uma nova sessão ou modificar uma sessão existente para um alias de bot e o ID de usuário	Gravar	bot alias*		
RecognizeText	Concede permissão para enviar a colaboração do usuário (somente em texto) para um alias de bot	Gravar	bot alias*		
RecognizeUtterance	Concede permissão para enviar a colaboração do usuário (texto ou fala) para um alias de bot	Gravar	bot alias*		
SearchAssociatedTranscripts	Concede permissão para pesquisar transcrições associadas que atendem aos critérios especificados	Lista	bot*		
StartBotRecommendation	Concede permissão para iniciar uma recomendação de bot para um local de bot existente	Gravar	bot*		
StartBotResourceGeneration	Concede permissão para iniciar uma geração de recurso para um local de bot existente	Gravar	bot*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartConversation	Concede permissão para transmitir a entrada do usuário (speech/text/DTMF) para um alias de bot	Gravar	bot alias*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartImport	Concede permissão para iniciar uma nova importação com o arquivo de importação carregado	Gravar	bot		lex:CreateBot lex:CreateBotLocale lex:CreateCustomVocabulary lex:CreateIntent lex:CreateSlot lex:CreateSlotType lex:CreateTestSet lex:DeleteBotLocale lex:DeleteCustomVocabulary lex:DeleteIntent

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					lex:DeleteSlot lex:DeleteSlotType lex:UpdateBot lex:UpdateBotLocale lex:UpdateCustomVocabulary lex:UpdateIntent lex:UpdateSlot lex:UpdateSlotType lex:UpdateTestSet
			bot alias		
			test set		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
StartTestExecution	Concede permissão para iniciar uma execução de teste usando um conjunto de testes	Gravar	test set*		
StartTestSetGeneration	Concede permissão para gerar um conjunto de testes	Gravar	test set		
StopBotRecommendation	Concede permissão para parar uma recomendação de bot para um local de bot existente	Gravar	bot*		
TagResource	Concede permissão para adicionar ou substituir etiquetas de um recurso Lex	Marcação	bot		
			bot alias		
			test set		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource		Marcação	bot		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	Concede permissão para remover etiquetas de um recurso do Lex.		bot alias		
			test set		
				aws:TagKeys	
UpdateBot	Concede permissão para atualizar um bot existente	Gravação	bot*		
UpdateBotAlias	Concede permissão para atualizar uma alias de bot existente	Gravação	bot alias*		
UpdateBotLocale	Concede permissão para atualizar um local de bot existente	Gravar	bot*		
UpdateBotRecommendation	Concede permissão para atualizar uma solicitação de recomendação de bot existente	Gravar	bot*		
UpdateCustomVocabulary [somente permissão]	Concede permissão para atualizar um vocabulário personalizado existente	Gravar	bot*		
UpdateExport	Concede permissão para atualizar uma exportação existente	Gravação	bot*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateIntent	Concede permissão para atualizar uma intenção existente	Gravação	bot*		
UpdateResourcePolicy	Concede permissão para atualizar uma política de recursos existente para um recurso do Lex	Gravação	bot		
			bot alias		
UpdateSlot	Concede permissão para atualizar um slot existente	Gravação	bot*		
UpdateSlotType	Concede permissão para atualizar um tipo de slot existente	Gravar	bot*		
UpdateTestSet	Concede permissão para atualizar um conjunto de testes existente	Gravar	test set*		

Tipos de recursos definidos pelo Amazon Lex V2

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do Amazon Lex V2

O Amazon Lex V2 define as chaves de condição a seguir que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas anexadas a um recurso do Lex.	String
aws:TagKeys	Filtra o acesso pelo conjunto de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS License Manager

AWS O License Manager (prefixo do serviço:`license-manager`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS License Manager
- Tipos de recursos definidos pelo AWS License Manager
- Chaves de condição do AWS License Manager

Ações definidas pelo AWS License Manager

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptGrant	Concede permissão para aceitar uma concessão	Write	grant*		
CheckInLicense	Concede permissão para fazer o check-in de direitos de licença de volta ao pool	Write			
CheckoutBorrowLicense	Concede permissão para verificar os direitos de licença para caso de uso de empréstimo	Write	license*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CheckoutLicense	Concede permissão para verificar os direitos de licença	Write			
CreateGrant	Concede permissão para criar uma nova concessão para licença	Write	license*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateGrantVersion	Concede permissão para criar nova versão de concessão	Write	grant*		
CreateLicense	Concede permissão para criar uma nova licença	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicenseConfiguration	Concede permissão para criar uma nova configuração de licença	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicenseConversionTaskForResource	Concede permissão para criar uma tarefa de conversão de licença para um recurso	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateLicenseManagerReportGenerator	Concede permissão para criar um gerador de relatórios para uma configuração de licença.	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicenseVersion	Concede permissão para criar nova versão da licença	Gravar	license*		
CreateToken	Concede permissão para criar um novo token para licença	Gravar	license*		
DeleteGrant	Concede permissão para excluir uma concessão	Gravar	grant*		
DeleteLicense	Concede permissão para excluir uma licença	Write	license*		
DeleteLicenseConfiguration	Concede permissão para excluir permanentemente uma configuração de licença	Write	license-configuration*		
DeleteLicenseManagerReportGenerator	Concede permissão para excluir um gerador de relatórios.	Write	report-generator*		
DeleteToken	Concede permissão para excluir token	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ExtendLicenseConsumption	Concede permissão para estender o período de consumo de direitos de licença já finalizados	Write			
GetAccessToken	Concede permissão para obter o token de acesso	Read			
GetGrant	Concede permissão para obter um subsídio	Read	grant*		
GetLicense	Concede permissão para obter uma licença	Read	license*		
GetLicenseConfiguration	Concede permissão para obter uma configuração de licença	Leitura	license-configuration*		
GetLicenseConversionTask	Concede permissão para recuperar uma tarefa de conversão de licença	Leitura			
GetLicenseManagerReportGenerator	Concede permissão para obter um gerador de relatórios.	Read	report-generator*		
GetLicenseUsage	Concede permissão para obter um uso de licença	Read	license*		
GetServiceSettings	Concede permissão para obter configurações de serviço	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAssociationsForLicenseConfiguration	Concede permissão para listar associações para uma configuração de licença selecionada	List	license-configuration*		
ListDistributedGrants	Concede permissão para listar concessões distribuídas	List			
ListFailuresForLicenseConfigurationOperations	Concede permissão para listar as operações de configuração de licença que falharam	List	license-configuration*		
ListLicenseConfigurations	Concede permissão para listar configurações de licença	Leitura			
ListLicenseConversionTasks	Concede permissão para listar as tarefas de conversão de licença	Lista			
ListLicenseManagerReportGenerators	Concede permissão para listar geradores de relatórios.	List	license-configuration		
ListLicenseSpecificationsForResource	Concede permissão para listar especificações de licença associadas a um recurso selecionado	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListLicenseVersions	Concede permissão para listar versões de licença	List	license*		
ListLicenses	Concede permissão para listar licenças	Leitura			
ListReceivedGrants	Concede permissão para listar concessões recebidas	Lista			
ListReceivedGrantsForOrganization	Concede permissão para listar concessões recebidas por organização	Lista			
ListReceivedLicenses	Concede permissão para listar licenças recebidas	Lista			
ListReceivedLicensesForOrganization	Concede permissão para listar licenças recebidas por organização	Lista			
ListResourceInventory	Concede permissão para listar inventário de recursos	List			
ListTagsForResource	Concede permissão para listar etiquetas para um recurso selecionado	Leitura	grant		
			license		
			license-configuration		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			report-generator		
ListTokens	Concede permissão para listar tokens	List			
ListUsageForLicenseConfiguration	Concede permissão para listar registros de uso para configuração de licença selecionada	List	license-configuration*		
RejectGrant	Concede permissão para rejeitar uma concessão	Write	grant*		
TagResource	Concede permissão para marcar um recurso selecionado	Marcação	grant		
			license		
			license-configuration		
			report-generator		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource		Marcação	grant		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	Concede permissão para desmarcar um recurso selecionado		license		
			license-configuration		
			report-generator		
				aws:TagKeys	
UpdateLicenseConfiguration	Concede permissão para atualizar uma configuração de licença existente	Write	license-configuration*		
UpdateLicenseManagerReportGenerator	Concede permissão para atualizar um gerador de relatórios para uma configuração de licença.	Write	report-generator*		
UpdateLicenseSpecificationsForResource	Concede permissão para atualizar especificações de licença para um recurso selecionado	Write	license-configuration*		
UpdateServiceSettings	Concede permissão para atualizações de configurações de serviço	Permissions management			

Tipos de recursos definidos pelo AWS License Manager

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
license-configuration	`arn:${Partition}:license-manager:${Region}:${Account}:license-configuration:${LicenseConfigurationId}`	aws:ResourceTag/${TagKey} license-manager:ResourceTag/${TagKey}
license	`arn:${Partition}:license-manager::${Account}:license:${LicenseId}`	aws:ResourceTag/${TagKey}
grant	`arn:${Partition}:license-manager::${Account}:grant:${GrantId}`	aws:ResourceTag/${TagKey}
report-generator	`arn:${Partition}:license-manager:${Region}:${Account}:report-generator:${ReportGeneratorId}`	aws:ResourceTag/${TagKey} license-manager:ResourceTag/${TagKey}

Chaves de condição do AWS License Manager

AWS O License Manager define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves de etiqueta que são transmitidas na solicitação	ArrayOfString
license-manager:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String

Ações, recursos e chaves de condição para o AWS License Manager Linux Subscriptions Manager

AWS O License Manager Linux Subscriptions Manager (prefixo do serviço:`license-manager-linux-subscriptions`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS License Manager Linux Subscriptions Manager
- Tipos de recursos definidos pelo AWS License Manager Linux Subscriptions Manager
- Chaves de condição para o AWS License Manager Linux Subscriptions Manager

Ações definidas pelo AWS License Manager Linux Subscriptions Manager

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeregisterSubscriptionProvider	Concede permissão para excluir permanentemente um provedor de assinatura no AWS License Manager	Gravar	subscription-provider*		
GetRegisteredSubscriptionProvider	Concede permissão para obter um provedor de assinatura no AWS License Manager	Leitura	subscription-provider*		
GetServiceSettings	Concede permissão para obter as configurações de serviço para assinaturas Linux no AWS License Manager	Leitura			
ListLinuxSubscriptionInstances	Concede permissão para listar todas as instâncias com assinaturas Linux no License Manager AWS	Leitura			
ListLinuxSubscriptions	Concede permissão para listar todas as assinaturas Linux no License Manager AWS	Leitura			
ListRegisteredSubscriptionProviders	Concede permissão para listar provedores de assinatura no AWS License Manager	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar etiquetas para um recurso selecionado	Leitura	subscription-provider*		
RegisterSubscriptionProvider	Concede permissão para criar um novo provedor de assinatura no AWS License Manager	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Concede permissão para marcar um recurso selecionado	Marcação	subscription-provider*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso selecionado	Tags	subscription-provider*		
				aws:TagKeys	
UpdateServiceSettings	Concede permissão para atualizar as configurações de serviço para assinaturas Linux no AWS License Manager	Gravar			

Tipos de recursos definidos pelo AWS License Manager Linux Subscriptions Manager

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
subscription-provider	`arn:${Partition}:license-manager-linux-subscriptions:${Region}:${Account}:subscription-provider/${SubscriptionProviderId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o AWS License Manager Linux Subscriptions Manager

AWS O License Manager Linux Subscriptions Manager define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String

Chaves de condição	Descrição	Tipo
aws:TagKeys	Filtra o acesso pelas chaves de etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS License Manager User Subscriptions

AWS As assinaturas de usuário do License Manager (prefixo do serviço:`license-manager-user-subscriptions`) fornecem os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS License Manager User Subscriptions
- Tipos de recursos definidos pelo AWS License Manager User Subscriptions
- Chaves de condição para o AWS License Manager User Subscriptions

Ações definidas pelo AWS License Manager User Subscriptions

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o

nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
Associate User	Concede permissão para associar um usuário registrado a uma instância iniciada com	Gravar	identity-provider*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	produtos de assinaturas de usuário do gerenciador de licenças			aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicenseServerEndpoint	Concede permissão para criar um endpoint de servidor de licenças para um determinado tipo de servidor para um determinado provedor de identidade	Gravar	identity-provider*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteLicenseServerEndpoint	Concede permissão para excluir um endpoint do servidor de licenças para um determinado tipo de servidor para um determinado provedor de identidade	Gravar	identity-provider*		
			license-server-endpoint*		
DeregisterIdentityProvider	Concede permissão para cancelar o registro do Microsoft Active Directory license-manager-user-subscriptions para um produto	Gravar	identity-provider*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateUser	Concede permissão para desassociar um usuário registrado de uma instância iniciada com produtos de assinaturas de usuário do gerenciador de licenças	Gravar	identity-provider* instance-user*		
ListIdentityProviders	Concede permissão para listar todos os provedores de identidade assinaturas de usuário do gerenciador de licenças	Lista			
ListInstances	Concede permissão para listar todas as instâncias iniciadas com produtos de assinaturas de usuário do gerenciador de licenças	Lista			
ListLicenseServerEndpoints	Concede permissão para listar endpoints do servidor de licenças	Lista			
ListProductSubscriptions	Concede permissão para listar todas as assinaturas de produtos para um produto e um provedor de identidades	Lista	identity-provider*		
ListTagsForResource	Concede permissão para listar etiquetas para um recurso selecionado	Leitura	identity-provider* instance-user*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			license-server-endpoint*		
			product-subscription*		
ListUserAssociations	Concede permissão para listar todos os usuários associados a uma instância iniciada para um produto	Lista	identity-provider*		
RegisterIdentityProvider	Concede permissão para registrar o Microsoft Active Directory em um produto license-manager-user-subscriptions	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
StartProductSubscription	Concede permissão para iniciar assinatura de produto para um usuário em um Active Directory registrado para um produto	Gravar	identity-provider*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopProductSubscription	Concede permissão para interromper assinatura de produto para um usuário em um Active Directory registrado para um produto	Gravar	identity-provider*		
			product-subscription*		
TagResource	Concede permissão para marcar um recurso selecionado	Marcação	identity-provider*		
			instance-user*		
			license-server-endpoint*		
			product-subscription*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso selecionado	Tags	identity-provider*		
			instance-user*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			license-server-endpoint*		
			product-subscription*		
UpdateIdentityProviderSettings	Concede permissão para atualizar a configuração do provedor de identidade	Gravar	identity-provider*		

Tipos de recursos definidos pelo AWS License Manager User Subscriptions

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
	`:product-subscription/${ProductSubscriptionId}`	
instance-user	`arn:${Partition}:license-manager-user-subscriptions:${Region}:${Account}:instance-user/${InstanceUserId}`	aws:ResourceTag/${TagKey}
license-server-endpoint	`arn:${Partition}:license-manager-user-subscriptions:${Region}:${Account}:license-server-endpoint/${LicenseServerEndpointId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o AWS License Manager User Subscriptions

AWS As assinaturas de usuário do License Manager definem as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves de etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Lightsail

O Amazon Lightsail (prefixo do serviço: `lightsail`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Lightsail
- Tipos de recursos definidos pelo Amazon Lightsail
- Chaves de condição do Amazon Lightsail

Ações definidas pelo Amazon Lightsail

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AllocateStaticIp	Concede permissão para criar um endereço IP estático que pode ser associado a uma instância	Gravar			
AttachCertificateToDistribution	Concede permissão para anexar um SSL/TLS certificado à sua distribuição da rede de distribuição de conteúdo (CDN) do Amazon Lightsail	Gravar	Certificate* Distribution*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AttachDisk	Concede permissão para anexar um disco a uma instância	Write	Disk*		
AttachInstancesToLoadBalancer	Concede permissão para associar uma ou mais instâncias a um balanceador de carga	Write	LoadBalancer*		
AttachLoadBalancerTlsCertificate	Concede permissão para associar um certificado TLS a um balanceador de carga	Write	LoadBalancer*		
AttachStaticIp	Concede permissão para associar um endereço IP estático a uma instância	Write	Instance* StaticIp*		
CloseInstancePublicPorts	Concede permissão para fechar uma porta pública de uma instância	Gravar	Instance*		
CopySnapshot	Concede permissão para copiar um snapshot de um Região da AWS para outro no Amazon Lightsail	Gravar			
CreateBucket	Concede permissão para criar um bucket do Amazon Lightsail	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateBucketAccessKey	Concede permissão para criar uma nova chave de acesso para o bucket especificado	Gravar	Bucket*		
CreateCertificate	Concede permissão para criar um SSL/TLS certificado	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	lightsail:CreateDomainEntry lightsail:GetDomains
CreateCloudFormationStack	Concede permissão para criar uma nova EC2 instância da Amazon a partir de um snapshot exportado do Amazon Lightsail	Gravar			
CreateContactMethod	Concede permissão para criar um método de contato por e-mail ou mensagem de texto SMS	Write			
CreateContainerService	Concede permissão para criar um serviço de contêiner do Amazon Lightsail	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateContainerServiceDeployment	Concede permissão para criar uma implantação para seu serviço de contêiner do Amazon Lightsail	Write	ContainerService*		
CreateContainerServiceRegistryLogin	Concede permissão para criar um conjunto temporário de credenciais de login que você pode usar para fazer login no processo Docker em sua máquina local	Write			
CreateDisk	Concede permissão para criar um disco	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDiskFromSnapshot	Concede permissão para criar um disco a partir do snapshot	Write	DiskSnapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDiskSnapshot	Concede permissão para criar um snapshot do disco	Write	Disk		
			Instance		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDistribution	Concede permissão para criar uma distribuição de rede de entrega de conteúdo (CDN) do Amazon Lightsail	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDomain	Concede permissão para criar um recurso de domínio para o nome de domínio especificado	Write		aws:RequestTag/${TagKey} aws:TagKeys	route53:DeleteHostedZone route53:GetHostedZone route53:ListHostedZonesByName route53domains:GetDomainDetail route53domains:GetOperationDetail route53domains:ListDomains route53domains:ListOperations route53domains:Upd

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ateDomainNameservers
CreateDomainEntry	Concede permissão para criar uma ou mais entradas de registro DNS para um recurso de domínio: endereço (A), nome canônico (CNAME), mail exchanger (MX), servidor de nome (NS), início de autoridade (SOA), localizador de serviço (SRV) ou texto (TXT)	Gravar	Domain*		
CreateGUISessionAccessDetails	Concede permissão para criar URLs que são usadas para acessar a sessão de interface gráfica do usuário (GUI) de uma instância	Gravar	Instance*		
CreateInstanceSnapshot	Concede permissão para criar o snapshot de uma instância	Write	Instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateInstances	Concede permissão para criar uma ou mais instâncias	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateInstancesFromSnapshot	Concede permissão para criar uma ou mais instâncias com base em um snapshot de instância	Write	InstanceSnapshot*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateKeyPair	Concede permissão para criar um par de chaves usado para autenticar e conectar a uma instância	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLoadBalancer	Concede permissão para criar um balanceador de carga	Write		aws:RequestTag/${TagKey} aws:TagKeys	lightsail:CreateDomainEntry lightsail:GetDomains

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateLoadBalancerTlsCertificate	Concede permissão para criar um certificado TLS de um balanceador de carga	Write	LoadBalancer*		lightsail:CreateDomainEntry lightsail:GetDomains
CreateRelationalDatabase	Concede permissão para criar um novo banco de dados relacional	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRelationalDatabaseFromSnapshot	Concede permissão para criar um banco de dados relacional com base em um snapshot	Write	RelationalDatabaseSnapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRelationalDatabaseSnapshot	Concede permissão para criar um snapshot de um banco de dados relacional	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteAlarm	Concede permissão para excluir um alarme	Write	Alarm*		
DeleteAutoSnapshot	Concede permissão para excluir um snapshot automático de uma instância ou disco	Write			
DeleteBucket	Concede permissão para excluir um bucket do Amazon Lightsail	Write	Bucket*		
DeleteBucketAccessKey	Concede permissão para excluir uma chave de acesso para o bucket do Amazon Lightsail especificado	Gravar	Bucket*		
DeleteCertificate	Concede permissão para excluir um SSL/TLS certificado	Gravar	Certificate*		
DeleteContactMethod	Concede permissão para excluir um método de contato	Write			
DeleteContainerImage	Concede permissão para excluir uma imagem de contêiner registrada no seu serviço de contêiner do Amazon Lightsail	Write	ContainerService*		
DeleteContainerService	Concede permissão para excluir seu serviço de contêiner do Amazon Lightsail	Write	ContainerService*		
DeleteDisk	Concede permissão para excluir um disco	Write	Disk*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteDiskSnapshot	Concede permissão para excluir um snapshot de disco	Write	DiskSnapshot*		
DeleteDistribution	Concede permissão para excluir sua distribuição de rede de entrega de conteúdo (CDN) do Amazon Lightsail	Write	Distribution*		
DeleteDomain	Concede permissão para excluir um recurso de domínio e todos os seus registros DNS	Write	Domain*		
DeleteDomainEntry	Concede permissão para excluir uma entrada de registro DNS de um recurso de domínio	Write	Domain*		
DeleteInstance	Concede permissão para excluir uma instância	Write	Instance*		
DeleteInstanceSnapshot	Concede permissão para excluir um snapshot de instância	Write	InstanceSnapshot*		
DeleteKeyPair	Concede permissão para excluir um par de chaves usado para autenticar e conectar a uma instância	Write	KeyPair*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteKnownHostKeys	Concede permissão para excluir a chave ou o certificado do host conhecido usado pelos clientes SSH ou RDP baseados em navegador do Amazon Lightsail para autenticar uma instância	Write	Instance*		
DeleteLoadBalancer	Concede permissão para excluir um balanceador de carga	Write	LoadBalancer*		
DeleteLoadBalancerTlsCertificate	Concede permissão para excluir um certificado TLS de um balanceador de carga	Write	LoadBalancer*		
DeleteRelationalDatabase	Concede permissão para excluir um banco de dados relacional	Write	RelationalDatabase*		
DeleteRelationalDatabaseSnapshot	Concede permissão para excluir um snapshot de banco de dados relacional	Gravar	RelationalDatabaseSnapshot*		
DetachCertificateFromDistribution	Concede permissão para separar um SSL/TLS certificado da sua distribuição da rede de distribuição de conteúdo (CDN) do Amazon Lightsail	Gravar	Distribution*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DetachDisk	Concede permissão para desassociar um disco de uma instância	Write	Disk*		
DetachInstancesFromLoadBalancer	Concede permissão para desassociar uma ou mais instâncias de um balanceador de carga	Write	LoadBalancer*		
DetachStaticIp	Concede permissão para desassociar um IP estático de uma instância à qual ele está associado	Write	StaticIp*		
DisableAddOn	Concede permissão para desabilitar um complemento para um recurso do Amazon Lightsail	Gravar			
DownloadDefaultKeyPair	Concede permissão para baixar o par de chaves padrão usado para autenticar e se conectar a instâncias em um determinado Região da AWS	Gravar			
EnableAddOn	Concede permissão para habilitar ou modificar um complemento para um recurso do Amazon Lightsail	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ExportSnapshot	Concede permissão para exportar um snapshot do Amazon Lightsail para a Amazon EC2	Gravar	DiskSnapshot		iam:CreateServiceLinkedRole iam:PutRolePolicy
			InstanceSnapshot		
GetActiveNames	Concede permissão para obter os nomes de todos os recursos ativos (não excluídos)	Read			
GetAlarms	Concede permissão para exibir informações sobre os alarmes configurados	Read			
GetAutoSnapshots	Concede permissão para exibir os instantâneos automáticos disponíveis para uma instância ou disco	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetBlueprints	Concede permissão para obter uma lista de imagens de instância, ou blueprints. É possível usar um blueprint para criar uma nova instância executando um sistema operacional específico, bem como uma pilha de desenvolvimento ou aplicativo pré-instalado. O software executado em sua instância depende do blueprint que você define ao criar a instância	Leitura			
GetBucketAccessKeys	Concede permissão para obter a chave de acesso existente IDs para o bucket especificado do Amazon Lightsail	Leitura			
GetBucketBundles	Concede permissão para obter os pacotes que podem ser aplicados a um bucket do Amazon Lightsail	Read			
GetBucketMetricData	Concede permissão para obter os pontos de dados de uma métrica específica para um bucket do Amazon Lightsail	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetBuckets	Concede permissão para obter informações sobre um ou mais buckets do Amazon Lightsail	Read			
GetBundles	Concede permissão para obter uma lista de pacotes de instâncias. É possível usar um pacote para criar uma nova instância com um conjunto de especificações de performance, como conetiquetaem de CPU, tamanho de disco, tamanho de RAM e franquia de transferência de rede. O custo da instância depende do pacote que você define ao criar a instância	Leitura			
GetCertificates	Concede permissão para visualizar informações sobre um ou mais certificados do Amazon Lightsail SSL/TLS	Leitura			
GetCloudFormationStackRecords	Concede permissão para obter informações sobre todas as CloudFormation pilhas usadas para criar EC2 recursos da Amazon a partir de snapshots exportados do Amazon Lightsail	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetContactMethods	Concede permissão para visualizar informações sobre os métodos de contato configurados	Read			
GetContainerAPIMetadata	Concede permissão para exibir informações sobre contêineres do Amazon Lightsail, como a versão atual do plugin Lightsail Control (lightsailctl)	Read			
GetContainerImages	Concede permissão para visualizar as imagens de contêiner registradas no seu serviço de contêiner do Amazon Lightsail	Read			
GetContainerLog	Concede permissão para visualizar os eventos de log de um contêiner do seu serviço de contêiner do Amazon Lightsail	Read			
GetContainerServiceDeployments	Concede permissão para visualizar as implantações do seu serviço de contêiner do Amazon Lightsail	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetContainerServiceMetricData	Concede permissão para visualizar os pontos de dados de uma métrica específica do seu serviço de contêiner do Amazon Lightsail	Read			
GetContainerServicePowers	Concede permissão para visualizar a lista de poderes que podem ser especificados para seus serviços de contêiner do Amazon Lightsail	Read			
GetContainerServices	Concede permissão para visualizar informações sobre um ou mais dos seus serviços de contêiner do Amazon Lightsail	Leitura			
GetCostEstimate	Concede permissão para obter as informações sobre o custo estimado de um recurso especificado	Leitura	Disk Instance		
GetDisk	Concede permissão para obter informações sobre um disco	Read			
GetDiskSnapshot	Concede permissão para obter informações sobre um snapshot de disco	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetDiskSnapshots	Concede permissão para obter informações sobre todos os snapshots de disco	Read			
GetDisks	Concede permissão para obter informações sobre todos os discos	Read			
GetDistributionBundles	Concede permissão para exibir a lista de pacotes que podem ser aplicados às suas distribuições da rede de entrega de conteúdo (CDN) do Amazon Lightsail	Read			
GetDistributionLatestCacheReset	Concede permissão para exibir o carimbo de data/hora e o status da última redefinição de cache de uma distribuição específica da rede de entrega de conteúdo (CDN) do Amazon Lightsail	Read			
GetDistributionMetricData	Concede permissão para visualizar os pontos de dados de uma métrica específica para uma distribuição de rede de entrega de conteúdo (CDN) do Amazon Lightsail	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetDistributions	Concede permissão para visualizar informações sobre uma ou mais distribuições da rede de entrega de conteúdo (CDN) do Amazon Lightsail	Read			
GetDomain	Concede permissão para obter registros DNS para um recurso de domínio	Read			
GetDomains	Concede permissão para obter registros DNS para todos os recurso de domínio	Leitura			
GetExportSnapshotRecords	Concede permissão para obter informações sobre todos os registros de snapshots exportados do Amazon Lightsail para a Amazon EC2	Leitura			
GetInstance	Concede permissão para obter informações sobre uma instância	Read			
GetInstanceAccessDetails	Concede permissão para obter chaves temporárias que podem ser usadas para autenticar e conectar a uma instância	Write	Instance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetInstanceMetricData	Concede permissão para obter os pontos de dados da métrica especificada de uma instância	Read			
GetInstancePortStates	Concede permissão para obter o status das portas de uma instância	Read			
GetInstanceSnapshot	Concede permissão para obter informações sobre um snapshot de instância	Read			
GetInstanceSnapshots	Concede permissão para obter informações sobre todos os snapshots de instâncias	Read			
GetInstanceState	Concede permissão para obter o estado de uma instância	Read			
GetInstances	Concede permissão para obter informações sobre todas as instâncias	Read			
GetKeyPair	Concede permissão para obter informações sobre um par de chaves	Read			
GetKeyPairs	Concede permissão para obter informações sobre todos os pares de chaves	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetLoadBalancer	Concede permissão para obter informações sobre um balanceador de carga	Leitura			
GetLoadBalancerMetricData	Concede permissão para obter os pontos de dados da métrica especificada de um balanceador de carga	Read			
GetLoadBalancerTlsCertificates	Concede permissão para obter informações sobre os certificados TLS de um balanceador de carga	Leitura			
GetLoadBalancerTlsPolicies	Concede permissão para obter uma lista de políticas de segurança TLS que você pode aplicar aos balanceadores de carga do Lightsail	Leitura			
GetLoadBalancers	Concede permissão para obter informações sobre balanceadores de carga	Read			
GetOperation	Concede permissão para obter informações sobre uma operação. As operações incluem eventos, como quando você cria uma instância, aloca um IP estático, associa um IP estático e assim por diante	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetOperations	Concede permissão para obter informações sobre todas as operações. As operações incluem eventos, como quando você cria uma instância, aloca um IP estático, associa um IP estático e assim por diante	Read			
GetOperationsForResource	Concede permissão para obter operações para um recurso	Leitura			
GetRegions	Concede permissão para obter uma lista de todos os itens válidos Regiões da AWS para o Amazon Lightsail	Leitura			
GetRelationalDatabase	Concede permissão para obter informações sobre um banco de dados relacional	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetRelationalDatabaseBlueprints	Concede permissão para obter uma lista de imagens de bancos de dados relacionais, ou blueprints. É possível usar um blueprint para criar um novo banco de dados que executa um mecanismo de banco de dados específico. O mecanismo de banco de dados que é executado no banco de dados depende do blueprint que você define ao criar o banco de dados relacional	Read			
GetRelationalDatabaseBundles	Concede permissão para obter uma lista de pacotes de bancos de dados relacionais. É possível usar um pacote para criar um novo banco de dados com um conjunto de especificações de performance, como conetiquetaem de CPU, tamanho de disco, tamanho de RAM, franquia de transferência de rede e padrão de alta disponibilidade. O custo do banco de dados depende do pacote que você define ao criar o banco de dados relacional	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetRelationalDatabaseEvents	Concede permissão para obter eventos de um banco de dados relacional	Read			
GetRelationalDatabaseLogEvents	Concede permissão para obter eventos do fluxo de log especificado de um banco de dados relacional	Read			
GetRelationalDatabaseLogStreams	Concede permissão para obter os fluxos de log disponíveis para um banco de dados relacional	Read			
GetRelationalDatabaseMasterUserPassword	Concede permissão para obter a senha do usuário primário de um banco de dados relacional	Write	RelationalDatabase*		
GetRelationalDatabaseMetricData	Concede permissão para obter os pontos de dados da métrica especificada de um banco de dados relacional	Read			
GetRelationalDatabaseParameters	Concede permissão para obter os parâmetros de um banco de dados relacional	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetRelationalDatabaseSnapshot	Concede permissão para obter informações sobre um snapshot de banco de dados relacional	Read			
GetRelationalDatabaseSnapshots	Concede permissão para obter informações sobre todos os snapshot de bancos de dados relacionais	Read			
GetRelationalDatabases	Concede permissão para obter informações sobre todos os bancos de dados relacionais	Leitura			
GetSetupHistory	Concede permissão para obter informações detalhadas das solicitações de configuração que foram executadas no recurso especificado	Leitura	Instance		
GetStaticIp	Concede permissão para obter informações sobre um IP estático	Leitura			
GetStaticIps	Concede permissão para obter informações sobre todas as estáticas IPs	Leitura			
ImportKeyPair	Concede permissão para importar uma chave pública de um par de chaves	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
IsVpcPeered	Concede permissão para obter um valor booleano que indica se a Virtual Private Cloud (VPC) do Amazon Lightsail está emparelhada	Read			
OpenInstancePublicPorts	Concede permissão para adicionar ou abrir uma porta pública de uma instância	Write	Instance*		
PeerVpc	Concede permissão para tentar emparelhar a Virtual Private Cloud (VPC) do Amazon Lightsail com a VPC padrão	Write			
PutAlarm	Concede permissão para criar ou atualizar um alarme e associá-lo à métrica especificada	Write	Alarm*		
PutInstancePublicPorts	Concede permissão para definir as portas abertas especificadas para uma instância e fecha todas as portas para cada protocolo não incluído na solicitação	Write	Instance*		
RebootInstance	Concede permissão para reinicializar uma instância que está em um estado de execução	Write	Instance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RebootRelationalDatabase	Concede permissão para reinicializar um banco de dados relacional que está em um estado de execução	Write	RelationalDatabase*		
RegisterContainerImage	Concede permissão para registrar uma imagem de contêiner no seu serviço de contêiner do Amazon Lightsail	Write	ContainerService*		
ReleaseStaticIp	Concede permissão para excluir um IP estático	Write	StaticIp*		
ResetDistributionCache	Concede permissão para excluir conteúdo atualmente armazenado em cache da sua distribuição de rede de entrega de conteúdo (CDN) do Amazon Lightsail	Write	Distribution*		
SendContactMethodVerification	Concede permissão para enviar uma solicitação de verificação para um método de contato por e-mail para garantir que ele seja de propriedade do solicitante	Write			
SetIpAddressType	Concede permissão para definir o tipo de endereço IP para um recurso do Amazon Lightsail	Write	Distribution		
			Instance		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			LoadBalancer		
SetResourceAccessForBucket	Concede permissão para definir os recursos do Amazon Lightsail que podem acessar o bucket do Amazon Lightsail especificado	Gravar	Bucket*		
			Instance*		
SetupInstanceHttps	Concede permissão para criar um SSL/TLS certificado e instalá-lo em uma instância especificada	Gravar	Instance*		lightsail:GetInstanceAccessDetails
StartGUISession	Concede permissão para iniciar uma sessão de interface gráfica do usuário (GUI) usada para acessar o sistema operacional ou aplicação de uma instância	Gravar	Instance*		
StartInstance	Concede permissão para iniciar uma instância que está em um estado interrompido	Write	Instance*		
StartRelationalDatabase	Concede permissão para iniciar um banco de dados relacional que está em um estado interrompido	Gravar	RelationalDatabase*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopGUISession	Concede permissão para terminar uma sessão de interface gráfica do usuário (GUI) usada para acessar o sistema operacional ou aplicação de uma instância	Gravar	Instance*		
StopInstance	Concede permissão para interromper uma instância que está em um estado de execução	Write	Instance*		
StopRelationalDatabase	Concede permissão para interromper um banco de dados relacional que está em um estado de execução	Write	RelationalDatabase*		
TagResource	Concede permissão para marcar um recurso	Marcação	Bucket		
			Certificate		
			ContainerService		
			Disk		
			DiskSnapshot		
			Distribution		
			Domain		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			Instance		
			InstanceSnapshot		
			KeyPair		
			LoadBalancer		
			RelationalDatabase		
			RelationalDatabaseSnapshot		
			StaticIp		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TestAlarm	Concede permissão para testar um alarme exibindo um banner no console do Amazon Lightsail ou se um acionador de notificação estiver configurado para o alarme especificado, enviando uma notificação ao protocolo de notificação	Write	Alarm*		
UnpeerVpc	Concede permissão para tentar desemparelhar a Virtual Private Cloud (VPC) do Amazon Lightsail da VPC padrão	Write			
UntagResource	Concede permissão para desmarcar um recurso	Marcação	Bucket		
			Certificate		
			ContainerService		
			Disk		
			DiskSnapshot		
			Distribution		
			Domain		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			Instance		
			InstanceSnapshot		
			KeyPair		
			LoadBalancer		
			RelationalDatabase		
			RelationalDatabaseSnapshot		
			StaticIp		
				aws:TagKeys	
UpdateBucket	Concede permissão para atualizar um bucket do Amazon Lightsail existente	Write	Bucket*		
UpdateBucketBundle	Concede permissão para atualizar o pacote, ou plano de armazenamento, de um bucket do Amazon Lightsail existente	Write	Bucket*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateContainerService	Concede permissão para atualizar a configuração do seu serviço de contêiner do Amazon Lightsail, como seus nomes de poder, escala e domínio público	Write	ContainerService*		
UpdateDistribution	Concede permissão para atualizar uma distribuição de rede de entrega de conteúdo (CDN) existente do Amazon Lightsail ou sua configuração	Write	Distribution*		
UpdateDistributionBundle	Concede permissão para atualizar o pacote de sua distribuição de rede de entrega de conteúdo (CDN) do Amazon Lightsail	Write	Distribution*		
UpdateDomainEntry	Concede permissão para atualizar o recordset de um domínio após sua criação	Gravar	Domain*		
UpdateInstanceMetadataOptions	Concede permissão para atualizar as opções de metadados de uma instância	Gravar	Instance*		
UpdateLoadBalancerAttribute	Concede permissão para atualizar um atributo do balanceador de carga, como o caminho da verificação de integridade e a perdurabilidade da sessão	Write	LoadBalancer*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateRelationalDatabase	Concede permissão para atualizar um banco de dados relacional	Write	RelationalDatabase*		
UpdateRelationalDatabaseParameters	Concede permissão para atualizar os parâmetros de um banco de dados relacional	Write	RelationalDatabase*		

Tipos de recursos definidos pelo Amazon Lightsail

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Tipos de recursos	ARN	Chaves de condição
StaticIp	arn:${Partition}:lightsail:${Region}:${Account}:StaticIp/${Id}	aws:ResourceTag/${TagKey}
Disk	arn:${Partition}:lightsail:${Region}:${Account}:Disk/${Id}	aws:ResourceTag/${TagKey}
DiskSnapshot	arn:${Partition}:lightsail:${Region}:${Account}:DiskSnapshot/${Id}	aws:ResourceTag/${TagKey}
LoadBalancer	arn:${Partition}:lightsail:${Region}:${Account}:LoadBalancer/${Id}	aws:ResourceTag/${TagKey}
LoadBalancerTlsCertificate	arn:${Partition}:lightsail:${Region}:${Account}:LoadBalancerTlsCertificate/${Id}	
ExportSnapshotRecord	arn:${Partition}:lightsail:${Region}:${Account}:ExportSnapshotRecord/${Id}	
CloudFormationStackRecord	arn:${Partition}:lightsail:${Region}:${Account}:CloudFormationStackRecord/${Id}	
RelationalDatabase	arn:${Partition}:lightsail:${Region}:${Account}:RelationalDatabase/${Id}	aws:ResourceTag/${TagKey}
RelationalDatabaseSnapshot	arn:${Partition}:lightsail:${Region}:${Account}:RelationalDatabaseSnapshot/${Id}	aws:ResourceTag/${TagKey}
Alarm	arn:${Partition}:lightsail:${Region}:${Account}:Alarm/${Id}	
Certificate	arn:${Partition}:lightsail:${Region}:${Account}:Certificate/${Id}	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do Amazon Lightsail

O Amazon Lightsail define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por um par de chave valor da etiqueta que é permitido na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso por um par de chave e valor da etiqueta de um recurso.	Segmento
aws:TagKeys	Filtra o acesso por uma lista de chaves da etiqueta que são permitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o Amazon Location

O Amazon Location (prefixo de serviço: `geo`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em IAM políticas de permissão.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Location
- Tipos de recursos definidos pelo Amazon Location
- Chaves de condição para o Amazon Location

Ações definidas pelo Amazon Location

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateTrackerConsumer	Concede permissão para criar uma associação entre uma coleção de geocerca e um recurso de rastreador	Write	tracker*		
BatchDeleteDevicePositionHistory	Concede permissão para excluir um lote de históricos de posição do dispositivo de um recurso do monitor	Write	tracker*		
				geo:DeviceIds	
BatchDeleteGeofence	Concede permissão para excluir um lote de geocercas de uma coleção de geocercas	Write	geofence-collection*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				geo:GeofenceIds	
BatchEvaluateGeofences	Concede permissão para avaliar as posições do dispositivo em relação à posição de geocercas em uma determinada coleção de geocercas	Write	geofence-collection*		
BatchGetDevicePosition	Concede permissão para enviar uma solicitação de lote para recuperar posições do dispositivo	Read	tracker*		
				geo:DeviceIds	
BatchPutGeofence	Concede permissão para enviar uma solicitação de lote para adicionar geocercas a uma determinada coleção de geocerca	Write	geofence-collection*		
				geo:GeofenceIds	
BatchUpdateDevicePosition	Concede permissão para carregar uma atualização de posição para um ou mais dispositivos para um recurso de rastreador	Write	tracker*		
				geo:DeviceIds	
CalculateRoute	Concede permissão para calcular rotas usando um determinado recurso da calculadora de rotas	Leitura	route-calculator*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CalculateRouteMatrix	Concede permissão para calcular uma tabela de rotas usando um recurso de calculadora de uma determinada rota	Leitura	route-calculator*		
CreateGeofenceCollection	Concede permissão para criar uma coleção de geocerca	Gravar	geofence-collection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateKey	Concede permissão para criar um recurso de chave de API	Gravar	api-key*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMap	Concede permissão para criar um recurso de mapa	Write	map*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreatePlaceIndex	Concede permissão para criar um recurso de índice de lugar	Write	place-index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRouteCalculator	Concede permissão para criar um recurso de calculadora de rotas	Write	route-calculator*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTracker	Concede permissão para criar um recurso de rastreador	Write	tracker*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteGeofenceCollection	Concede permissão para excluir uma coleção de cerca geográfica	Gravar	geofence-collection*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteKey	Concede permissão para excluir um recurso de chave de API	Gravar	api-key*		
DeleteMap	Concede permissão para excluir um recurso de mapa	Write	map*		
DeletePlaceIndex	Concede permissão para excluir um recurso de índice de local	Write	place-index*		
DeleteRouteCalculator	Concede permissão para excluir um recurso de calculadora de rotas	Write	route-calculator*		
DeleteTracker	Concede permissão para excluir um recurso de rastreador	Write	tracker*		
DescribeGeofenceCollection	Concede permissão para recuperar detalhes de uma coleção de cerca geográfica	Leitura	geofence-collection*		
DescribeKey	Concede permissão para recuperar detalhes e o segredo do recurso de chave de API	Leitura	api-key*		
DescribeMap	Concede permissão para recuperar detalhes de um recurso de mapa	Read	map*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribePlaceIndex	Concede permissão para recuperar detalhes de um recurso de índice de lugar	Read	place-index*		
DescribeRouteCalculator	Concede permissão para recuperar detalhes do recurso de calculadora de rotas	Read	route-calculator*		
DescribeTracker	Concede permissão para recuperar detalhes de recursos de um rastreador	Read	tracker*		
DisassociateTrackerConsumer	Concede permissão para remover a associação entre um recurso de rastreador e uma coleção de geocerca	Gravar	tracker*		
ForecastGeofenceEvents	Concede permissão para prever eventos de cercas geográficas armazenadas em uma determinada coleção de cercas geográficas	Leitura	geofence-collection*		
GetDevicePosition	Concede permissão para recuperar a posição mais recente do dispositivo	Leitura	tracker*		
				geo:DeviceIds	
GetDevicePositionHistory	Concede permissão para recuperar o histórico da posição do dispositivo	Leitura	tracker*		
				geo:DeviceIds	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetGeofence	Concede permissão para recuperar os detalhes da cerca geográfica de uma coleção de cercas geográficas	Leitura	geofence-collection*		
				geo:GeofenceIds	
GetMapGlyphs	Concede permissão para recuperar o arquivo de glifo para um recurso de mapa	Read	map*		
GetMapSprites	Concede permissão para recuperar o arquivo sprite de um recurso de mapa	Read	map*		
GetMapStyleDescriptor	Concede permissão para recuperar o descritor de estilo de mapa de um recurso de mapa	Read	map*		
GetMapTile	Concede permissão para recuperar o bloco do mapa do recurso do mapa	Leitura	map*		
GetPlace	Concede permissão para encontrar um lugar por meio de seu ID exclusivo	Leitura	place-index*		
ListDevicePositions	Concede permissão para recuperar uma lista de dispositivos e suas posições mais recentes do recurso de monitor fornecido	Leitura	tracker*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListGeofenceCollections	Concede permissão para listas de coleções de geocerca	List	geofence-collection*		
ListGeofences	Concede permissão para listar geocercas armazenadas em uma determinada coleção de geocerca	Leitura	geofence-collection*		
ListKeys	Concede permissão para listar recursos de chave de API	Lista	api-key*		
ListMaps	Concede permissão para listar recursos de mapa	List	map*		
ListPlaceIndexes	Concede permissão para devolver uma lista de recursos de índice de lugar	List	place-index*		
ListRouteCalculators	Concede permissão para retornar uma lista de recursos da calculadora de rotas	List	route-calculator*		
ListTagsForResource	Concede permissão para listar as etiquetas (metadados) que você atribuiu ao recurso	Read	api-key		
			geofence-collection		
			map		
			place-index		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			route-calculator		
			tracker		
ListTrackerConsumers	Concede permissão para recuperar uma lista de coleções de geocerca atualmente associadas ao recurso de rastreador fornecido	Read	tracker*		
ListTrackers	Concede permissão para retornar uma lista de recursos do rastreador	List	tracker*		
PutGeofence	Concede permissão para adicionar uma nova geocerca ou atualizar uma geocerca existente para uma determina da coleção de geocerca	Write	geofence-collection*		
				geo:GeofenceIds	
SearchPlaceIndexForPosition	Concede permissão para reverter geocódigos em uma determinada coordenada	Leitura	place-index*		
SearchPlaceIndexForSuggestions	Concede permissão para gerar sugestões de endereços e pontos de interesse com base em texto em formato livre parcial ou com erros de ortografia	Leitura	place-index*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SearchPlaceIndexForText	Concede permissão para geocodificar texto em formato livre, como endereço, nome, cidade ou região	Read	place-index*		
TagResource	Concede permissão para adicionar ou modificar as etiquetas do recurso fornecido. Etiquetas são metadados que podem ser usados para gerenciar um recurso	Marcação	api-key		
			geofence-collection		
			map		
			place-index		
			route-calculator		
			tracker		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover as etiquetas fornecidas (metadados) do recurso	Tags	api-key		
			geofence-collection		
			map		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			place-index		
			route-calculator		
			tracker		
				aws:TagKeys	
UpdateGeofenceCollection	Concede permissão para atualizar uma coleção de cercas geográficas	Gravar	geofence-collection*		
UpdateKey	Concede permissão para atualizar um recurso de chave de API	Gravar	api-key*		
UpdateMap	Concede permissão para atualizar um recurso de mapa	Gravar	map*		
UpdatePlaceIndex	Concede permissão para atualizar um recurso de índice de local	Gravar	place-index*		
UpdateRouteCalculator	Concede permissão para atualizar um recurso de calculadora de rotas	Gravar	route-calculator*		
UpdateTracker	Concede permissão para atualizar um recurso de rastreador	Gravar	tracker*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
VerifyDevicePosition	Concede permissão para verificar a posição de um dispositivo	Leitura	tracker*		
				geo:DeviceIds	

Tipos de recursos definidos pelo Amazon Location

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Tipos de recursos	ARN	Chaves de condição
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

Chaves de condição para o Amazon Location

O Amazon Location define as chaves de condição a seguir que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso pela chave e valor de uma etiqueta em uma solicitação	String
aws:ResourceTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta em uma solicitação	ArrayOfString
geo:DeviceIds	Filtra acessos pela presença de ids de dispositivos na solicitação	ArrayOfString

Chaves de condição	Descrição	Type
geo:GeofenceIds	Filtra acessos pela presença de ids de geocercas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para Amazon Location Service Maps

O Amazon Location Service Maps (prefixo do serviço:`geo-maps`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Location Service Maps
- Tipos de recursos definidos pelo Amazon Location Service Maps
- Chaves de condição para Amazon Location Service Maps

Ações definidas pelo Amazon Location Service Maps

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetStaticMap	Concede permissão para recuperar o mapa estático	Leitura	provider*		
GetTile	Concede permissão para recuperar o bloco do mapa	Leitura	provider*		

Tipos de recursos definidos pelo Amazon Location Service Maps

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
provider	`arn:${Partition}:geo-maps:${Region}: :provider/default`	

Chaves de condição para Amazon Location Service Maps

O Geo Maps não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para Amazon Location Service Places

O Amazon Location Service Places (prefixo do serviço:`geo-places`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Location Service Places

- Tipos de recursos definidos pelo Amazon Location Service Places
- Chaves de condição para Amazon Location Service Places

Ações definidas pelo Amazon Location Service Places

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
Autocomplete	Concede permissão para preencher automaticamente a entrada de texto com possíveis lugares e endereços à medida que o usuário digita	Leitura	provider*		
Geocode	Concede permissão para geocodificar um endereço textual ou lugar em coordenadas geográficas	Leitura	provider*		
GetPlace	Concede permissão para consultar um local por seu ID de local exclusivo	Leitura	provider*		
ReverseGeocode	Concede permissão para converter coordenadas geográficas em um endereço ou local legível por humanos	Leitura	provider*		
SearchNearby	Concede permissão para recuperar lugares próximos a uma posição que correspondam a um conjunto de restrições definidas pelo usuário, como categoria ou	Leitura	provider*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	tipo de alimento oferecido pelo local				
SearchText	Concede permissão para consultar lugares usando uma única entrada de texto de formato livre	Leitura	provider*		
Suggest	Concede permissão para sugerir lugares em potencial com base na opinião do usuário	Leitura	provider*		

Tipos de recursos definidos pelo Amazon Location Service Places

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
provider	`arn:${Partition}:geo-places:${Region}::provider/default`	

Chaves de condição para Amazon Location Service Places

O Geo Places não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para Amazon Location Service Routes

O Amazon Location Service Routes (prefixo do serviço:`geo-routes`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Location Service Routes
- Tipos de recursos definidos pelo Amazon Location Service Routes
- Chaves de condição para Amazon Location Service Routes

Ações definidas pelo Amazon Location Service Routes

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
Calculate Isolines	Concede permissão para determinar destinos ou áreas de serviço acessíveis dentro de um tempo especificado	Leitura	provider*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CalculateRouteMatrix	Concede permissão para calcular a matriz de roteamento que fornece o tempo de viagem e as distâncias entre conjuntos de origens e destinos	Leitura	provider*		
CalculateRoutes	Concede permissão para calcular rotas entre dois ou mais locais	Leitura	provider*		
OptimizeWaypoints	Concede permissão para calcular a sequência mais eficiente para visitar vários pontos de referência ou locais ao longo de uma rota	Leitura	provider*		
SnapToRoads	Concede permissão para aprimorar a precisão do posicionamento geográfico alinhando as coordenadas GPS aos segmentos de estrada mais próximos em um mapa digital	Leitura	provider*		

Tipos de recursos definidos pelo Amazon Location Service Routes

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves

são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
provider	`arn:${Partition}:geo-routes:${Region}::provider/default`	

Chaves de condição para Amazon Location Service Routes

O Geo Routes não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do Amazon Lookout for Equipment

O Amazon Lookout for Equipment (prefixo de serviço: `lookoutequipment`) fornece os recursos, ações e chaves de contexto de condição a seguir, específicos do serviço, para uso nas IAM políticas de permissão.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Lookout for Equipment
- Tipos de recursos definidos pelo Amazon Lookout for Equipment
- Chaves de condição para o Amazon Lookout for Equipment

Ações definidas pelo Amazon Lookout for Equipment

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando

usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDataset	Concede permissão para criar um conjunto de dados	Write	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInferenceScheduler	Concede permissão para criar um programador de inferências para um modelo treinado	Gravar	inference-scheduler*		
			model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLabel	Concede permissão para criar um rótulo	Gravar	label-group*		
CreateLabelGroup	Concede permissão para criar um grupo de rótulos	Gravar	label-group*		
				aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
CreateModel	Concede permissão para criar um modelo treinado em um conjunto de dados	Gravar	dataset*		
			model*		
			label-group		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRetrainingScheduler	Concede permissão para criar um programador de retreinamento para um modelo treinado	Gravar	model*		
DeleteDataset	Concede permissão para excluir um conjunto de dados	Write	dataset*		
DeleteInferenceScheduler	Concede permissão para excluir um programador de inferências	Gravar	inference-scheduler*		
DeleteLabel	Concede permissão para excluir um rótulo	Gravar	label-group*		
DeleteLabelGroup	Concede permissão para excluir um grupo de rótulos	Gravar	label-group*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteModel	Concede permissão para excluir um modelo	Gravar	model*		
DeleteResourcePolicy	Concede permissão para excluir uma política de recurso	Gravar	dataset		
			model		
			model-version		
DeleteRetrainingScheduler	Concede permissão para excluir um programador de retreinamento de um modelo treinado	Gravar	model*		
DescribeDataIngestionJob	Concede permissão para descrever um trabalho de ingestão de dados	Read			
DescribeDataset	Concede permissão para descrever um conjunto de dados	Read	dataset*		
DescribeInferenceScheduler	Concede permissão para descrever um programador de inferências	Leitura	inference-scheduler*		
DescribeLabelGroup	Concede permissão para descrever um grupo de rótulos	Leitura	label-group*		
DescribeModel	Concede permissão para descrever um modelo	Leitura	model*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeModelVersion	Concede permissão para descrever uma versão de modelo	Leitura	model-version*		
DescribeResourcePolicy	Concede permissão para descrever uma política de recurso	Leitura	dataset		
			model		
			model-version		
DescribeRetrainingScheduler	Concede permissão para descrever um programador de retreinamento de um modelo treinado	Leitura	model*		
DescribeLabel	Concede permissão para descrever um rótulo	Leitura	label-group*		
ImportDataset	Concede permissão para importar um conjunto de dados	Gravar	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ImportModelVersion	Concede permissão para importar uma versão de modelo	Gravar	dataset*		
			model*		
			label-group		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys lookoutequipment:IsImportingData	
ListDataIngestionJobs	Concede permissão para listar os trabalhos de ingestão de dados em sua conta ou para um conjunto de dados específico	List	dataset*		
ListDatasets	Concede permissão para listar os conjuntos de dados em sua conta	Lista			
ListInferenceEvents	Concede permissão para listar os eventos de inferência de um programador de inferências	Leitura	inference-scheduler*		
ListInferenceExecutions	Concede permissão para listar as execuções de inferência de um programador de inferências	Read	inference-scheduler*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListInferenceSchedulers	Concede permissão para listar os programadores de inferência em sua conta	Lista			
ListLabelGroups	Concede permissão para listar os grupos de rótulos em sua conta	Lista	label-group*		
ListLabels	Concede permissão para listar os rótulos de sua conta	Lista	label-group*		
ListModelVersions	Concede permissão para listar as versões de modelo na sua conta	Lista	model*		
ListModels	Concede permissão para listar os modelos na sua conta	Lista			
ListRetrainingSchedulers	Concede permissão para listar os programadores de retreinamento na sua conta	Lista			
ListSensorStatistics	Concede permissão para listar as estatísticas do sensor para um conjunto de dados ou um trabalho de ingestão específico	Lista	dataset*		
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	dataset		
			inference-scheduler		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			label-group		
			model		
			model-version		
PutResourcePolicy	Concede permissão para determinar uma política de recursos	Gravar	dataset		
			model		
			model-version		
StartDataIngestionJob	Concede permissão para iniciar um trabalho de ingestão de dados para um conjunto de dados	Write	dataset*		
StartInferenceScheduler	Concede permissão para iniciar um programador de inferências	Gravar	inference-scheduler*		
StartRetrainingScheduler	Concede permissão para iniciar um programador de retreinamento de um modelo treinado	Gravar	model*		
StopInferenceScheduler	Concede permissão para interromper um programador de inferências	Gravar	inference-scheduler*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopRetrainingScheduler	Concede permissão para interromper um programador de retreinamento de um modelo treinado	Gravar	model*		
TagResource	Concede permissão para marcar um recurso	Marcação	dataset		
			inference-scheduler		
			label-group		
			model		
			model-version		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso	Tags	dataset		
			inference-scheduler		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			label-group		
			model		
			model-version		
				aws:TagKeys	
UpdateActiveModelVersion	Concede permissão para definir a versão ativa do modelo para um determinado modelo de machine learning	Gravar	model*		
			model-version*		
UpdateInferenceScheduler	Concede permissão para atualizar um programador de inferências	Gravar	inference-scheduler*		
UpdateLabelGroup	Concede permissão para atualizar um grupo de rótulos	Gravar	label-group*		
UpdateModel	Concede permissão para atualizar um modelo treinado	Gravar	model*		
UpdateRetrainingScheduler	Concede permissão para atualizar um programador de retreinamento de um modelo treinado	Gravar	model*		

Tipos de recursos definidos pelo Amazon Lookout for Equipment

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição para o Amazon Lookout for Equipment

O Amazon Lookout for Equipment define as chaves de condição a seguir que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais

as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString
lookoutequipment:IsImportingData	Filtra o acesso com base na estratégia de importação dos dados subjacentes	Bool

Ações, recursos e chaves de condição do Amazon Lookout for Metrics

O Amazon Lookout for Metrics (prefixo de serviço: `lookoutmetrics`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Lookout for Metrics

- Tipos de recursos definidos pelo Amazon Lookout for Metrics
- Chaves de condição para o Amazon Lookout for Metrics

Ações definidas pelo Amazon Lookout for Metrics

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ActivateAnomalyDetector	Concede permissão para ativar um detector de anomalias	Write	AnomalyDetector*		
BackTestAnomalyDetector	Concede permissão para executar um teste retroativo com um detector de anomalias	Write	AnomalyDetector*		
CreateAlert	Concede permissão para criar um alerta para um detector de anomalias	Write	Alert*		
			AnomalyDetector*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAnomalyDetector	Concede permissão para criar um detector de anomalias	Write	AnomalyDetector*		
				aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
CreateMetricSet	Concede permissão para criar um conjunto de dados	Gravar	AnomalyDetector*		
			MetricSet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeactivateAnomalyDetector	Concede permissão para desativar um detector de anomalias	Gravar	AnomalyDetector*		
DeleteAlert	Concede permissão para excluir um alerta.	Write	Alert*		
DeleteAnomalyDetector	Concede permissão para excluir um detector de anomalias	Write	AnomalyDetector*		
DescribeAlert	Concede permissão para obter detalhes sobre um alerta	Read	Alert*		
DescribeAnomalyDetectionExecutions	Concede permissão para obter informações sobre um trabalho de detecção de anomalias	Read	AnomalyDetector*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeAnomalyDetector	Concede permissão para obter detalhes sobre um detector de anomalias	Read	AnomalyDetector*		
DescribeMetricSet	Concede permissão para obter detalhes sobre um conjunto de dados	Leitura	MetricSet*		
DetectMetricSetConfig	Concede permissão para detectar a configuração do conjunto de métricas da origem dos dados	Gravar	AnomalyDetector*		
GetAnomalyGroup	Concede permissão para obter detalhes sobre um grupo de métricas afetadas	Read	AnomalyDetector*		
GetDataQualityMetrics	Concede permissão para obter métricas de qualidade de dados para um detector de anomalias	Read	AnomalyDetector*		
GetFeedback	Concede permissão para obter feedback sobre métricas afetadas para um grupo de anomalias	Read	AnomalyDetector*		
GetSampleData	Concede permissão para obter uma seleção de registros de amostra de uma fonte de dados do Amazon S3	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAlerts	Concede permissão para obter uma lista de alertas para um detector	List	AnomalyDetector		
ListAnomalyDetectors	Concede permissão para obter uma lista de detectores de anomalias	Lista			
ListAnomalyGroupRelatedMetrics	Concede permissão para obter uma lista de medidas relacionadas em um grupo de anomalias	Lista	AnomalyDetector*		
ListAnomalyGroupSummaries	Concede permissão para obter uma lista de grupos de anomalias	List	AnomalyDetector*		
ListAnomalyGroupTimeSeries	Concede permissão para obter uma lista de métricas afetadas para uma medida em um grupo de anomalias	List	AnomalyDetector*		
ListMetricSets	Concede permissão para obter uma lista de conjuntos de dados	List	AnomalyDetector		
ListTagsForResource	Concede permissão para obter uma lista de etiquetas para um detector, conjunto de dados ou alerta	Read	Alert		
			AnomalyDetector		
			MetricSet		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutFeedback	Concede permissão para adicionar feedback para uma métrica afetada em um grupo de anomalias	Write	AnomalyDetector*		
TagResource	Concede permissão para adicionar etiquetas a um detector, conjunto de dados ou alerta	Marcação	Alert		
			AnomalyDetector		
			MetricSet		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permissão para remover etiquetas de um detector, conjunto de dados ou alerta	Tags	Alert		
			AnomalyDetector		
			MetricSet		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateAlert	Concede permissão para atualizar um alerta para um detector de anomalias	Gravar	Alert*		
UpdateAnomalyDetector	Concede permissão para atualizar um detector de anomalias	Write	AnomalyDetector*		
UpdateMetricSet	Concede permissão para atualizar um conjunto de dados	Write	MetricSet*		

Tipos de recursos definidos pelo Amazon Lookout for Metrics

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
AnomalyDetector	`arn:${Partition}:lookoutmetrics:${Region}:${Account}:AnomalyDetector:${AnomalyDetectorName}`	aws:ResourceTag/${TagKey}
MetricSet	`arn:${Partition}:lookoutmetrics:${Region}:${Account}:MetricSet/${AnomalyDetectorName}/${MetricSetName}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
Alert	`arn:${Partition}:lookoutmetrics:${Region}:${Account}:Alert:${AlertName}`	aws:ResourceTag/${TagKey}

Chaves de condição para o Amazon Lookout for Metrics

O Amazon Lookout for Metrics define as chaves de condição a seguir que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Lookout for Vision

O Amazon Lookout for Vision (prefixo de serviço: `lookoutvision`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em IAM políticas de permissão.

Referências:

- Saiba como configurar este serviço.

- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Lookout for Vision
- Tipos de recursos definidos pelo Amazon Lookout for Vision
- Chaves de condição para o Amazon Lookout for Vision

Ações definidas pelo Amazon Lookout for Vision

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDataset	Concede permissão para criar um manifesto de conjunto de dados	Write			
CreateModel	Concede permissão para criar um novo modelo de detecção de anomalias	Write	model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProject	Concede permissão para criar um novo projeto	Write	project*		
DeleteDataset	Concede permissão para excluir um conjunto de dados	Write			
DeleteModel	Concede permissão para excluir um modelo e todos os ativos associados	Write	model*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteProject	Concede permissão para remover permanentemente um projeto	Write	project*		
DescribeDataset	Concede permissão para mostrar informações detalhadas sobre o manifesto do conjunto de dados	Read			
DescribeModel	Concede permissão para mostrar informações detalhadas sobre um modelo	Leitura	model*		
DescribeModelPackagingJob	Concede permissão para exibir informações detalhadas sobre um trabalho de empacotamento de modelos	Leitura			
DescribeProject	Concede permissão para mostrar informações detalhadas sobre um projeto	Read	project*		
DescribeTrialDetection [somente permissão]	Concede permissão para fornecer informações de estado sobre um trabalho de detecção de anomalias em execução	Read			
DetectAnomalies	Concede permissão para invocar a detecção de anomalias	Write	model*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDatasetEntries	Concede permissão para listar o conteúdo do manifesto do conjunto de dados	Leitura			
ListModelPackagingJobs	Concede permissão para listar todos os trabalhos de empacotamento de modelos associados a um projeto	Lista			
ListModels	Concede permissão para listar todos os modelos associados a um projeto	List			
ListProjects	Concede permissão para listar todos os projetos	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	model		
ListTrialDetections [somente permissão]	Concede permissão para listar todos os trabalhos de detecção de anomalias	List			
StartModel	Concede permissão para iniciar o modelo de detecção de anomalias	Gravar	model*		
StartModelPackagingJob	Concede permissão para iniciar um trabalho de empacotamento de modelos	Gravar	model*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartTrialDetection [somente permissão]	Concede permissão para iniciar a detecção em massa de anomalias para um conjunto de imagens armazenadas em um bucket do S3	Write			
StopModel	Concede permissão para interromper o modelo de detecção de anomalias	Gravar	model*		
TagResource	Concede permissão para marcar um recurso com determinados pares de chave-valor	Tags	model		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover a etiqueta com a chave fornecida de um recurso	Tags	model		
				aws:TagKeys	
UpdateDatasetEntries	Concede permissão para atualizar um manifesto de conjunto de dados de treinamento ou teste	Write			

Tipos de recursos definidos pelo Amazon Lookout for Vision

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
model	`arn:${Partition}:lookoutvision:${Region}:${Account}:model/${ProjectName}/${ModelVersion}`	aws:ResourceTag/${TagKey}
project	`arn:${Partition}:lookoutvision:${Region}:${Account}:project/${ProjectName}`	

Chaves de condição para o Amazon Lookout for Vision

O Amazon Lookout for Vision define as chaves de condição a seguir que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Machine Learning

O Amazon Machine Learning (prefixo do serviço: `machinelearning`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Machine Learning
- Tipos de recursos definidos pelo Amazon Machine Learning
- Chaves de condição do Amazon Machine Learning

Ações definidas pelo Amazon Machine Learning

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddTags	Adiciona uma ou mais etiquetas a um objeto, até um limite de 10. Cada etiqueta consiste em uma chave e um valor opcional	Marcação	batchprediction		
			datasource		
			evaluation		
			mlmodel		
CreateBatchPrediction	Gera previsões para um grupo de observações	Gravar	batchprediction*		
			datasource*		
			mlmodel*		
CreateDataSourceFromRDS	Cria um DataSource objeto a partir de um Amazon RDS	Gravar	datasource*		
CreateDataSourceFromRedshift	Cria um DataSource a partir de um banco de dados hospedado em um cluster do Amazon Redshift	Gravar	datasource*		
CreateDataSourceFromS3	Cria um DataSource objeto a partir do S3	Gravar	datasource*		
CreateEvaluation	Cria uma nova avaliação de um MLModel	Gravar	datasource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			evaluation*		
			mlmodel*		
CreateMLModel	Cria um novo MLModel	Gravar	datasource*		
			mlmodel*		
CreateRealtimeEndpoint	Cria um endpoint em tempo real para o MLModel	Gravar	mlmodel*		
DeleteBatchPrediction	Atribui o status EXCLUÍDO a um BatchPrediction, tornando-o inutilizável	Gravar	batchprediction*		
DeleteDataSource	Atribui o status EXCLUÍDO a um DataSource, tornando-o inutilizável	Gravar	datasource*		
DeleteEvaluation	Atribui o status DELETED (EXCLUÍDO) a uma avaliação tornando-a inutilizável	Gravar	evaluation*		
DeleteMLModel	Atribui o status EXCLUÍDO a um MLModel, tornando-o inutilizável	Gravar	mlmodel*		
DeleteRealtimeEndpoint	Exclui um endpoint em tempo real de um MLModel	Gravar	mlmodel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteTags	Exclui as etiquetas especificadas associadas a um objeto ML. Após essa operação ser concluída, você não pode recuperar etiquetas excluídas	Tags	batchprediction		
			datasource		
			evaluation		
			mlmodel		
DescribeBatchPredictions	Retorna uma lista de BatchPrediction operações que correspondem aos critérios de pesquisa na solicitação	Lista			
DescribeDataSources	Retorna uma lista das DataSource que correspondem aos critérios de pesquisa na solicitação	Lista			
DescribeEvaluations	Retorna uma lista das DescribeEvaluations que correspondem aos critérios de pesquisa na solicitação	Lista			
DescribeMLModels	Retorna uma lista das MLModel que correspondem aos critérios de pesquisa na solicitação	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeTags	Descreve uma ou mais etiquetas para o objeto do Amazon ML	Lista	batchprediction		
			datasource		
			evaluation		
			mlmodel		
GetBatchPrediction	Retorna um BatchPrediction que inclui metadados detalhados, status e informações do arquivo de dados	Leitura	batchprediction*		
GetDataSource	Retorna um DataSource que inclui metadados e informações do arquivo de dados, bem como o status atual do DataSource	Leitura	datasource*		
GetEvaluation	Retorna uma avaliação que inclui metadados, bem como o status atual da avaliação	Leitura	datasource*		
GetMLModel	Retorna um MLModel que inclui metadados detalhados e informações da fonte de dados, bem como o status atual do MLModel	Leitura	mlmodel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
Predict	Gera uma previsão da observação usando o modelo do ML especificado	Gravar	mlmodel*		
UpdateBatchPrediction	Atualiza o BatchPredictionName de um BatchPrediction	Gravar	batchprediction*		
UpdateDataSource	Atualiza o DataSourceName de um DataSource	Gravar	datasource*		
UpdateEvaluation	Atualiza o EvaluationName de uma avaliação	Gravar	evaluation*		
UpdateMLModel	Atualiza o MLModel nome e o ScoreThreshold de um MLModel	Gravar	mlmodel*		

Tipos de recursos definidos pelo Amazon Machine Learning

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
batchprediction	`arn:${Partition}:machinelearning:${Region}:${Account}:batchprediction/${BatchPredictionId}`	
datasource	`arn:${Partition}:machinelearning:${Region}:${Account}:datasource/${DatasourceId}`	
evaluation	`arn:${Partition}:machinelearning:${Region}:${Account}:evaluation/${EvaluationId}`	
mlmodel	`arn:${Partition}:machinelearning:${Region}:${Account}:mlmodel/${MlModelId}`	

Chaves de condição do Amazon Machine Learning

O Machine Learning não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do Amazon Macie

O Amazon Macie (prefixo do serviço: `macie2`) fornece os recursos, as ações e as chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Macie
- Tipos de recursos definidos pelo Amazon Macie
- Chaves de condição do Amazon Macie

Ações definidas pelo Amazon Macie

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de

recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

> **Note**
>
> As GetMasterAccount ações DisassociateFromMasterAccount e foram descontinuadas. Em vez disso, recomendamos que você especifique as GetAdministratorAccount ações DisassociateFromAdministratorAccount e, respectivamente.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptInvitation	Concede permissão para aceitar um convite de associação do Amazon Macie	Write			
BatchGetCustomDataIdentifiers	Concede permissão para recuperar informações sobre um ou mais identificadores de dados personalizados	Leitura	CustomDataIdentifier*		
BatchUpdateAutomatedDiscoveryAccounts	Concede permissão a um administrador do Amazon Macie para alterar o status da descoberta automatizada de dados confidenciais para uma ou mais contas na organização	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAllowList	Concede permissão para criar e definir as configurações de uma lista de permissões	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateClassificationJob	Concede permissão para criar e definir as configurações de um trabalho de descoberta de dados sigilosos	Write	ClassificationJob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomDataIdentifier	Concede permissão para criar e definir as configurações de um identificador de dados personalizado	Write	CustomDataIdentifier*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFindingsFilter	Concede permissão para criar e definir as configurações de um filtro de descobertas	Write	FindingsFilter*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInvitations	Concede permissão para enviar um convite de associação do Amazon Macie	Write			
CreateMember	Concede permissão para associar uma conta a uma conta de administrador do Amazon Macie	Write	Member*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSampleFindings	Concede permissão para criar exemplos de descobertas	Write			
DeclineInvitations	Concede permissão para recusar convites de associação ao Amazon Macie	Gravar			
DeleteAllowList	Concede permissão para excluir uma lista de permissões	Gravar	AllowList*		
DeleteCustomDataIdentifier	Concede permissão para excluir um identificador de dados personalizado	Write	CustomDataIdentifier*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteFindingsFilter	Concede permissão para excluir um filtro de descobertas	Write	FindingsFilter*		
DeleteInvitations	Concede permissão para excluir convites de associação do Amazon Macie	Write			
DeleteMember	Concede permissão para excluir a associação entre uma conta e uma conta de administrador do Amazon Macie	Write	Member*		
DescribeBuckets	Concede permissão para recuperar dados estatísticos e outras informações sobre buckets do S3 monitorados e analisados pelo Amazon Macie	Read			
DescribeClassificationJob	Concede permissão para recuperar informações sobre o status e as configurações de um trabalho de descoberta de dados sigilosos	Leitura	ClassificationJob*		
DescribeOrganizationConfiguration	Concede permissão para recuperar informações sobre as configurações do Amazon Macie para uma organização AWS	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisableMacie	Concede permissão para desabilitar uma conta do Amazon Macie, que também exclui recursos do Macie para a conta	Gravar			
DisableOrganizationAdminAccount	Concede permissão para desativar uma conta como conta delegada de administrador do Amazon Macie para uma organização AWS	Gravar			
DisassociateFromAdministratorAccount	Concede a uma conta-membro do Amazon Macie permissão para se desassociar da conta de administrador do Macie	Gravar			
DisassociateFromMasterAccount	Concede a uma conta-membro do Amazon Macie permissão para se desassociar da conta de administrador do Macie	Gravar			
DisassociateMember	Concede a uma conta de administrador do Amazon Macie permissão para se desassociar de uma conta-membro do Macie	Gravar	Member*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
EnableMacie	Concede permissão para habilitar e especificar as configurações de uma nova conta do Amazon Macie	Gravar			
EnableOrganizationAdminAccount	Concede permissão para habilitar uma conta como conta delegada de administrador do Amazon Macie para uma organização AWS	Gravar			
GetAdministratorAccount	Concede permissão para recuperar informações sobre a conta de administrador do Amazon Macie para uma conta	Leitura			
GetAllowList	Concede permissão para recuperar as configurações e o status de uma lista de permissões	Leitura	AllowList*		
GetAutomatedDiscoveryConfiguration	Concede permissão para recuperar as definições de configuração e o status da descoberta automatizada de dados confidenciais de uma conta de administrador, organização ou conta autônoma do Amazon Macie	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetBucketStatistics	Concede permissão para recuperar dados estatísticos agregados para todos os buckets do S3 monitorados e analisados pelo Amazon Macie	Read			
GetClassificationExportConfiguration	Concede permissão para recuperar as configurações para exportar resultados de descobertas de dados sigilosos	Leitura			
GetClassificationScope	Concede permissão para recuperar as configurações do escopo de classificação de uma conta	Leitura			
GetCustomDataIdentifier	Concede permissão para recuperar informações sobre as configurações de um identificador de dados personalizado	Read	CustomDataIdentifier*		
GetFindingStatistics	Concede permissão para recuperar dados estatísticos agregados sobre descobertas	Read			
GetFindings	Concede permissão para recuperar os detalhes de uma ou mais descobertas	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetFindingsFilter	Concede permissão para recuperar informações sobre as configurações de um filtro de descobertas	Leitura	FindingsFilter*		
GetFindingsPublicationConfiguration	Concede permissão para recuperar as configurações para publicar descobertas no AWS Security Hub	Leitura			
GetInvitationsCount	Concede permissão para recuperar a contagem de convites de associação do Amazon Macie que foram recebidos por uma conta	Read			
GetMacieSession	Concede permissão para recuperar informações sobre o status e as configurações de uma conta do Amazon Macie	Leitura			
GetMasterAccount	Concede permissão para recuperar informações sobre a conta de administrador do Amazon Macie para uma conta	Leitura			
GetMember	Concede permissão para recuperar informações sobre uma conta associada a uma conta de administrador do Amazon Macie	Leitura	Member*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetResourceProfile	Concede permissão para recuperar estatísticas de descoberta de dados confidenciais e a pontuação de confidencialidade de um bucket do S3	Leitura			
GetRevealConfiguration	Concede permissão para recuperar o status e as configurações para recuperação de ocorrências de dados sigilosos informados por descobertas	Leitura			
GetSensitiveDataOccurrences	Concede permissão para recuperar ocorrências de dados sigilosos informados por descobertas	Leitura			
GetSensitiveDataOccurrencesAvailability	Concede permissão para verificar se as ocorrências de dados sigilosos podem ser recuperadas de uma descoberta	Leitura			
GetSensitivityInspectionTemplate	Concede permissão para recuperar as configurações do modelo de inspeção de confidencialidade de uma conta	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetUsageStatistics	Concede permissão para recuperar cotas e dados de uso agregados para uma ou mais contas	Read			
GetUsageTotals	Concede permissão para recuperar dados de uso agregados de uma conta	Leitura			
ListAllowLists	Concede permissão para recuperar um subconjunto informações sobre todas as listas de permissão de uma conta	Lista			
ListAutomatedDiscoveryAccounts	Concede permissão para recuperar o status da descoberta automatizada de dados confidenciais de uma conta	Lista			
ListClassificationJobs	Concede permissão para recuperar um subconjunto informações sobre o status e as configurações de um ou mais trabalhos de descoberta de dados sigilosos	Lista			
ListClassification Scopes	Concede permissão para recuperar um subconjunto informações sobre o escopo de classificação de uma conta	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListCustomDataIdentifiers	Concede permissão para recuperar informações sobre todos os identificadores de dados personalizados	List			
ListFindings	Concede permissão para recuperar um subconjunto de informações sobre uma ou mais descobertas	List			
ListFindingsFilters	Concede permissão para recuperar informações sobre todos os filtros de descobertas	List			
ListInvitations	Concede permissão para recuperar informações sobre todos os convites de associação do Amazon Macie que foram recebidos por uma conta	Lista			
ListManagedDataIdentifiers	Concede permissão para recuperar informações sobre os identificadores de dados gerenciados	Lista			
ListMembers	Concede permissão para recuperar informações sobre as contas-membro do Amazon Macie que estão associadas a uma conta de administrador do Macie	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListOrganizationAdminAccounts	Concede permissão para recuperar informações sobre a conta delegada de administrador do Amazon Macie para uma organização AWS	Lista			
ListResourceProfileArtifacts	Concede permissão para recuperar informações sobre objetos selecionados pelo Amazon Macie em um bucket do S3 para descoberta automatizada de dados confidenciais	Lista			
ListResourceProfileDetections	Concede permissão para recuperar informações sobre os tipos e a quantidade de dados confidenciais que o Amazon Macie encontrou em um bucket do S3	Lista			
ListSensitivityInspectionTemplates	Concede permissão para recuperar um subconjunto de informações sobre o modelo de inspeção de confidencialidade de uma conta	Lista			
ListTagsForResource	Concede permissão para recuperar as etiquetas de um recurso do Amazon Macie	Read	AllowList ClassificationJob		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			CustomDataIdentifier		
			FindingsFilter		
			Member		
PutClassificationExportConfiguration	Concede permissão para criar ou atualizar as configurações para armazenar resultados de descoberta de dados sigilosos	Gravar			
PutFindingsPublicationConfiguration	Concede permissão para atualizar as configurações para publicar descobertas no AWS Security Hub	Gravar			
SearchResources	Concede permissão para recuperar dados estatísticos e outras informações sobre AWS recursos que o Amazon Macie monitora e analisa	Leitura			
TagResource	Concede permissão para adicionar ou atualizar as etiquetas de um recurso do Amazon Macie	Marcação	AllowList		
			ClassificationJob		
			CustomDataIdentifier		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			FindingsFilter		
			Member		
				aws:RequestTag/${TagKey} aws:TagKeys	
TestCustomDataIdentifier	Concede permissão para testar um identificador de dados personalizado	Write			
UntagResource	Concede permissão para remover etiquetas de um recurso do Amazon Macie	Tags	AllowList		
			ClassificationJob		
			CustomDataIdentifier		
			FindingsFilter		
			Member		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateAllowList	Concede permissão para atualizar as configurações de uma lista de permissões	Gravar	AllowList*		
UpdateAutomatedDiscoveryConfiguration	Concede permissão para alterar o status da descoberta automatizada de dados confidenciais para uma conta de administrador, organização ou conta autônoma do Amazon Macie	Gravar			
UpdateClassificationJob	Concede permissão para alterar o status de um trabalho de descoberta de dados sigilosos	Gravar	ClassificationJob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateClassificationScope	Concede permissão para atualizar as configurações do escopo de classificação de uma conta	Gravar			
UpdateFindingsFilter	Concede permissão para atualizar as configurações de um filtro de descobertas	Gravar	FindingsFilter*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateMacieSession	Concede permissão a uma conta de administrador do Amazon Macie para suspender ou reativar o Macie para uma conta de membro	Gravar			
UpdateMemberSession	Concede a uma conta de administrador do Amazon Macie permissão para suspender ou reativar uma conta-membro do Macie	Gravar			
UpdateOrganizationConfiguration	Concede permissão para atualizar as configurações do Amazon Macie para uma organização AWS	Gravar			
UpdateResourceProfile	Concede permissão para atualizar a pontuação de confiabilidade de um bucket do S3	Gravar			
UpdateResourceProfileDetections	Concede permissão para atualizar as configurações de pontuação de confiabilidade de um bucket do S3	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateRevealConfiguration	Concede permissão para atualizar o status e as configurações para recuperação de ocorrências de dados sigilosos informados por descobertas	Gravar			
UpdateSensitivityInspectionTemplate	Concede permissão para atualizar as configurações do modelo de inspeção de confidencialidade de uma conta	Gravar			

Tipos de recursos definidos pelo Amazon Macie

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
AllowList	`arn:${Partition}:macie2:${Region}:${Account}:allow-list/${ResourceId}`	aws:ResourceTag/${TagKey}
ClassificationJob	`arn:${Partition}:macie2:${Region}:${Account}:classification-job/${ResourceId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
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}
Member	`arn:${Partition}:macie2:${Region}:${Account}:member/${ResourceId}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Macie

O Amazon Macie define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por um par de chave valor da etiqueta que é permitido na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso por um par de chave e valor da etiqueta de um recurso.	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Application Testing do AWS Mainframe Modernization

AWS O Mainframe Modernization Application Testing (prefixo do serviço:`apptest`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Application Testing do AWS Mainframe Modernization
- Tipos de recursos definidos pelo Application Testing do AWS Mainframe Modernization
- Chaves de condição do Application Testing do AWS Mainframe Modernization

Ações definidas pelo Application Testing do AWS Mainframe Modernization

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa

ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateTestCase	Concede permissão para criar um caso de teste	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTestConfiguration	Concede permissão para criar uma configuração de teste	Gravar		aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
CreateTestSuite	Concede permissão para criar um conjunto de testes	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteTestCase	Concede permissão para excluir um caso de testes	Gravar	TestCase*		
DeleteTestConfiguration	Concede permissão para excluir uma configuração de teste	Gravar	TestConfiguration*		
DeleteTestRun	Concede permissão para excluir uma execução de teste	Gravar	TestRun*		s3:DeleteObject s3:ListBucket
DeleteTestSuite	Concede permissão para excluir um conjunto de testes	Gravar	TestSuite*		
GetTestCase	Concede permissão para obter um caso de teste	Leitura	TestCase*		
GetTestConfiguration	Concede permissão para obter uma configuração de teste	Leitura	TestConfiguration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetTestRunStep	Concede permissão para obter a etapa de execução de teste	Leitura	TestRun*		
GetTestSuite	Concede permissão para obter um conjunto de testes	Leitura	TestSuite*		
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura			
ListTestCases	Concede permissão para listar casos de teste	Lista			
ListTestConfigurations	Concede permissão para listar configurações de teste	Lista			
ListTestRunSteps	Concede permissão para listar etapas para uma execução de teste	Leitura	TestRun*		
ListTestRunTestCases	Concede permissão para listar casos de teste para uma execução de teste	Leitura	TestRun*		
ListTestRuns	Concede permissão para listar execuções de testes	Lista			
ListTestSuites	Concede permissão para listar conjuntos de testes	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartTestRun	Concede permissão para iniciar uma execução de testes	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	cloudformation:CreateStack cloudformation:DeleteStack cloudformation:DescribeStacks dms:DescribeReplicationTasks dms:StartReplicationTask dms:StopReplicationTask ec2:DescribeAvailabilityZones ec2:DescribeVpcEndpointServ

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					iceConfigurations ec2:DescribeVpcEndpointServices m2:CreateDataSetImportTask m2:GetApplication m2:GetApplicationVersion m2:GetBatchJobExecution m2:GetDataSetDetails m2:GetDataSetImportTask m2:StartApplication

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					m2:StartBatchJob m2:StopApplication s3:CreateBucket s3:DeleteObject s3:GetObject s3:ListBucket s3:PutObject
TagResource	Concede permissão para marcar um recurso	Marcação	TestCase		
			TestConfiguration		
			TestRun		
			TestSuite		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso	Tags	TestCase		
			TestConfiguration		
			TestRun		
			TestSuite		
				aws:TagKeys	
UpdateTestCase	Concede permissão para atualizar um caso de teste	Gravar	TestCase*		
UpdateTestConfiguration	Concede permissão para atualizar uma configuração de teste	Gravar	TestConfiguration*		
UpdateTestSuite	Concede permissão para atualizar um conjunto de testes	Gravar	TestSuite*		

Tipos de recursos definidos pelo Application Testing do AWS Mainframe Modernization

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do Application Testing do AWS Mainframe Modernization

AWS O teste de aplicativos de modernização de mainframe define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por um par de chave valor da etiqueta que é permitido na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso por um par de chave e valor da etiqueta de um recurso.	Segmento
aws:TagKeys	Filtra o acesso por uma lista de chaves da etiqueta que são permitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS Mainframe Modernization Service

AWS O Mainframe Modernization Service (prefixo do serviço:`m2`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Mainframe Modernization Service
- Tipos de recursos definidos pelo AWS Mainframe Modernization Service
- Chaves de condição para o AWS Mainframe Modernization Service

Ações definidas pelo AWS Mainframe Modernization Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando

usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelBatchJobExecution	Concede permissão para cancelar a execução de um trabalho em lote	Gravar	Application*		
CreateApplication	Concede permissão para criar um aplicativo	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject s3:ListBucket
CreateDataSetExportTask	Concede permissão para criar uma tarefa de exportação de conjunto de dados	Gravar	Application*		s3:GetObject
CreateDataSetImportTask	Concede permissão para criar uma tarefa de importação de conjunto de dados	Gravar	Application*		s3:GetObject
CreateDeployment	Concede permissão para criar uma implantação	Gravar	Application*		elasticloadbalancing:AddTags elasticloadbalancing:CreateListener elasticloadbalancing:Create

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					TargetGroup elasticloadbalancing:RegisterTargets
			Environment		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateEnvironment	Concede permissão para criar um ambiente	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcs ec2:ModifyNetworkInterfaceAttribute

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					elasticfilesystem:DescribeMountTargets elasticloadbalancing:AddTags elasticloadbalancing:CreateLoadBalancer fsx:DescribeFileSystems iam:CreateServiceLinkedRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteApplication	Concede permissão para excluir um aplicativo	Gravar	Application*		elasticloadbalancing:DeleteListener elasticloadbalancing:DeleteTargetGroup
DeleteApplicationFromEnvironment	Concede permissão para excluir uma aplicação de um ambiente de runtime	Gravar	Application*		elasticloadbalancing:DeleteListener elasticloadbalancing:DeleteTargetGroup
DeleteEnvironment	Concede permissão para excluir um ambiente de runtime	Gravar	Environment*		elasticloadbalancing:DeleteLoadBalancer
GetApplication	Concede permissão para recuperar uma aplicação	Leitura	Application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetApplicationVersion	Concede permissão para recuperar uma versão de aplicação	Leitura	Application*		
GetBatchJobExecution	Concede permissão para recuperar a execução de um trabalho em lote	Leitura	Application*		
GetDataSetDetails	Concede permissão para recuperar detalhes de um conjunto de dados	Leitura	Application*		
GetDataSetExportTask	Concede permissão para exportar um conjunto de dados no local especificado do S3	Leitura	Application*		
GetDataSetImportTask	Concede permissão para recuperar uma tarefa de importação de conjunto de dados	Leitura	Application*		
GetDeployment	Concede permissão para recuperar uma implantação	Leitura	Application*		
GetEnvironment	Concede permissão para recuperar um ambiente de runtime	Leitura	Environment*		
GetSignedBluinsightsUrl	Concede permissão para criar um URL assinado do Bluinsights	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListApplicationVersions	Concede permissão para listar as versões de uma aplicação	Leitura	Application*		
ListApplications	Concede permissão para listar aplicações	Lista			
ListBatchJobDefinitions	Concede permissão para listar definições de trabalho em lote	Leitura	Application*		
ListBatchJobExecutions	Concede permissão para listar execuções de um trabalho em lote	Leitura	Application*		
ListBatchJobRestartPoints	Concede permissão para recuperar a execução de um trabalho em lote	Leitura	Application*		
ListDataSetExportHistory	Concede permissão para listar o histórico de exportação do conjunto de dados	Leitura	Application*		
ListDataSetImportHistory	Concede permissão para listar o histórico de importação de conjunto de dados	Leitura	Application*		
ListDataSets	Concede permissão para listar conjuntos de dados	Leitura	Application*		
ListDeployments	Concede permissão para listar implantações	Leitura	Application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListEngineVersions	Concede permissão para listar versões de mecanismo	Leitura			
ListEnvironments	Concede permissão para listar ambientes de runtime	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura			
StartApplication	Concede permissão para iniciar uma aplicação	Gravar	Application*		
StartBatchJob	Concede permissão para iniciar um trabalho em lote	Gravar	Application*		
StopApplication	Concede permissão para interromper uma aplicação	Gravar	Application*		
TagResource	Concede permissão para marcar um recurso	Marcação	Application		
			Environment		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso	Marcação	Application		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			Environment		
				aws:TagKeys	
UpdateApplication	Concede permissão para atualizar uma aplicação	Gravar	Application*		s3:GetObject s3:ListBucket
UpdateEnvironment	Concede permissão para atualizar um ambiente de runtime	Gravar	Environment*		

Tipos de recursos definidos pelo AWS Mainframe Modernization Service

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
Application	`arn:${Partition}:m2:${Region}:${Account}:app/${ApplicationId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
Environment	`arn:${Partition}:m2:${Region}:${Account}:env/${EnvironmentId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o AWS Mainframe Modernization Service

AWS O Mainframe Modernization Service define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por um par de chave valor da etiqueta que é permitido na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso por um par de chave e valor da etiqueta de um recurso.	Segmento
aws:TagKeys	Filtra o acesso por uma lista de chaves da etiqueta que são permitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Managed Blockchain

O Amazon Managed Blockchain (prefixo do serviço: `managedblockchain`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.

- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Managed Blockchain
- Tipos de recursos definidos pelo Amazon Managed Blockchain
- Chaves de condição do Amazon Managed Blockchain

Ações definidas pelo Amazon Managed Blockchain

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAccessor	Concede permissão para criar um acessador do Amazon Managed Blockchain	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
CreateMember	Concede permissão para criar um membro de uma rede do Amazon Managed Blockchain	Gravação	network*		iam:CreateServiceLinkedRole
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateNetwork	Concede permissão para criar uma rede do Amazon Managed Blockchain	Gravação		aws:TagKeys	iam:CreateServiceLinkedRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey}	
CreateNode	Concede permissão para criar um nó dentro de um membro de uma rede do Amazon Managed Blockchain	Gravação	member		iam:CreateServiceLinkedRole
			network		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateProposal	Concede permissão para criar uma proposta na qual outros membros da rede de blockchain podem votar para adicionar ou remover um membro em uma rede do Amazon Managed Blockchain	Gravar	network*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteAccessor	Concede permissão para excluir um acessador do Amazon Managed Blockchain	Gravar	accessor*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteMember	Concede permissão para excluir um membro e todos os recursos associados de uma rede do Amazon Managed Blockchain	Gravação	member*		
DeleteNode	Concede permissão para excluir um nó dentro de um membro de uma rede do Amazon Managed Blockchain	Gravar	node*		
GET [somente permissão]	Concede permissão para enviar solicitações HTTP GET para um nó do Ethereum	Gerenciamento de permissões			
GetAccessor	Concede permissão para retornar informações detalhadas sobre um acessador do Amazon Managed Blockchain	Leitura	accessor*		
GetMember	Concede permissão para retornar informações detalhadas sobre um membro de uma rede do Amazon Managed Blockchain	Leitura	member*		
GetNetwork	Concede permissão para retornar informações detalhadas sobre uma rede do Amazon Managed Blockchain	Leitura	network*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetNode	Concede permissão para retornar informações detalhadas sobre um nó dentro de um membro de uma rede do Amazon Managed Blockchain	Leitura	node*		
GetProposal	Concede permissão para retornar informações detalhadas sobre uma proposta de uma rede do Amazon Managed Blockchain	Leitura	proposal*		
Invoke [somente permissão]	Concede permissão para criar WebSocket conexões com um nó Ethereum	Gerenciamento de permissões			
InvokeRpcBitcoinMainnet	Concede permissão para invocar o Bitcoin Mainnet RPCs	Leitura			
InvokeRpcBitcoinTestnet	Concede permissão para invocar o Bitcoin Testnet RPCs	Leitura			
InvokeRpcPolygonMainnet	Concede permissão para invocar a Polygon Mainnet RPCs	Leitura			
InvokeRpcPolygonMumbaiTestnet	Concede permissão para invocar o Polygon Mumbai Testnet RPCs	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAccessors	Concede permissão para listar os acessadores do Amazon Managed Blockchain de propriedade da empresa atual Conta da AWS	Lista			
ListInvitations	Concede permissão para listar os convites estendidos aos ativos Conta da AWS de qualquer rede Blockchain Gerenciada	Lista			
ListMembers	Concede permissão para listar os membros de uma rede do Amazon Managed Blockchain e as propriedades de suas associações	Lista	network*		
ListNetworks	Concede permissão para listar as redes Amazon Managed Blockchain das quais o atual Conta da AWS participa	Lista			
ListNodes	Concede permissão para listar os nós dentro de um membro de uma rede do Amazon Managed Blockchain	List	member network		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListProposalVotes	Concede permissão para listar todos os votos de uma proposta, incluindo o valor do voto e o identificador exclusivo do membro que depositou o voto para a rede do Amazon Managed Blockchain específica	Leitura	proposal*		
ListProposals	Concede permissão para listar as propostas de uma rede do Amazon Managed Blockchain específica	List	network*		
ListTagsForResource	Concede permissão para visualizar as etiquetas associadas a um recurso do Amazon Managed Blockchain	Leitura	accessor		
			invitation		
			member		
			network		
			node		
			proposal		
POST [somente permissão]	Concede permissão para enviar solicitações HTTP POST para um nó do Ethereum	Gerenciamento de permissões			
RejectInvitation	Concede permissão para rejeitar o convite para participar da rede de blockchain	Gravação	invitation*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para adicionar etiquetas a um recurso do Amazon Managed Blockchain	Marcação	accessor		
			invitation		
			member		
			network		
			node		
			proposal		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover etiquetas de um recurso do Amazon Managed Blockchain	Marcação	accessor		
			invitation		
			member		
			network		
			node		
			proposal		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateMember	Concede permissão para atualizar um membro de uma rede do Amazon Managed Blockchain.	Gravação	member*		iam:CreateServiceLinkedRole
UpdateNode	Concede permissão para atualizar um nó dentro de um membro de uma rede do Amazon Managed Blockchain.	Gravação	node*		iam:CreateServiceLinkedRole
VoteOnProposal	Concede permissão para votar em uma proposta em nome do membro da rede de blockchain especificado	Gravação	proposal*		

Tipos de recursos definidos pelo Amazon Managed Blockchain

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
network	`arn:${Partition}:managedblockchain:${Region}::networks/${NetworkId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do Amazon Managed Blockchain

O Amazon Managed Blockchain define as chaves de condição a seguir que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra ações com base nas etiquetas transmitidas na solicitação	Segmento

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra ações com base nas etiquetas associadas a um recurso do Amazon Managed Blockchain	Segmento
aws:TagKeys	Filtra ações com base nas chaves da etiqueta transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Managed Blockchain Query

O Amazon Managed Blockchain Query (prefixo do serviço: `managedblockchain-query`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Managed Blockchain Query
- Tipos de recursos definidos pelo Amazon Managed Blockchain Query
- Chaves de condição do Amazon Managed Blockchain Query

Ações definidas pelo Amazon Managed Blockchain Query

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchGetTokenBalance	Concede permissão para chamadas em lote para a GetTokenBalance API	Leitura			
GetAssetContract	Concede permissão para buscar informações sobre um contrato no blockchain	Leitura			
GetTokenBalance	Concede permissão para recuperar o saldo de um token para um endereço no blockchain	Leitura			
GetTransaction	Concede permissão para recuperar uma transação no blockchain	Leitura			
ListAssetContracts	Concede permissão para buscar vários contratos no blockchain	Lista			
ListFilteredTransactionEvents	Concede permissão para recuperar eventos no blockchain com filtros adicionais	Lista			
ListTokenBalances	Concede permissão para recuperar vários saldos no blockchain	Listar			
ListTransactionEvents	Concede permissão para recuperar eventos em uma transação no blockchain	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTransactions	Concede permissão para recuperar várias transações em um blockchain	Lista			

Tipos de recursos definidos pelo Amazon Managed Blockchain Query

O Amazon Managed Blockchain não oferece suporte à especificação do ARN de um recurso no elemento `Resource` de uma instrução de política do IAM. Para permitir acesso ao Amazon Managed Blockchain Query, especifique `"Resource": "*"` na política.

Chaves de condição do Amazon Managed Blockchain Query

O Managed Blockchain Query não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o Amazon Managed Grafana

O Amazon Managed Grafana (prefixo de serviço: `grafana`) fornece os seguintes recursos, ações e chaves de contexto de condição, específicos do serviço, para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Managed Grafana
- Tipos de recursos definidos pelo Amazon Managed Grafana
- Chaves de condição para o Amazon Managed Grafana

Ações definidas pelo Amazon Managed Grafana

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateLicense	Concede permissão para fazer upgrade um espaço de trabalho com uma licença	Gravação	workspace*		aws-marketplace:ViewSubscriptions
CreateWorkspace	Concede permissão para criar um Workspace	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetManagedPrefixListEntries iam:CreateServiceLinkedRole organizations:DescribeOrganization sso:CreateManagedApplicationInstance

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					sso:DescribeRegisteredRegions sso:GetSharedSsoConfiguration
CreateWorkspaceApiKey	Concede permissão para criar chaves de API para um espaço de trabalho	Gravar	workspace*		
CreateWorkspaceServiceAccount	Concede permissão para criar contas de serviço para um espaço de trabalho	Gravar	workspace*		
CreateWorkspaceServiceAccountToken	Concede permissão para criar tokens de conta de serviço em um espaço de trabalho	Gravar	workspace*		
DeleteWorkspace	Concede permissão para excluir um Workspace	Gravar	workspace*		sso:DeleteManagedApplicationInstance
DeleteWorkspaceApiKey	Concede permissão para excluir chaves de API de um espaço de trabalho	Gravar	workspace*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteWorkspaceServiceAccount	Concede permissão para excluir contas de serviço em um espaço de trabalho	Gravar	workspace*		
DeleteWorkspaceServiceAccountToken	Concede permissão para excluir tokens de conta de serviço em um espaço de trabalho	Gravar	workspace*		
DescribeWorkspace	Concede permissão para descrever um Workspace	Leitura	workspace*		
DescribeWorkspaceAuthentication	Concede permissão para descrever os provedores de autenticação em um espaço de trabalho	Leitura	workspace*		
DescribeWorkspaceConfiguration	Concede permissão para descrever a string de configuração atual de um determinado espaço de trabalho	Leitura	workspace*		
DisassociateLicense	Concede permissão para remover uma licença de um espaço de trabalho	Gravação	workspace*		
ListPermissions	Concede permissão para listar as permissões em um espaço de trabalho	Listar	workspace*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar etiquetas associadas a um espaço de trabalho	Leitura	workspace		
ListVersions	Concede permissão para listar todas as versões do Grafana com suporte disponíveis. Opcionalmente, inclua um espaço de trabalho para listar as versões para as quais ele pode ser atualizado	Lista	workspace		
ListWorkspaceServiceAccountTokens	Concede permissão para listar tokens de conta de serviço em um espaço de trabalho	Leitura	workspace*		
ListWorkspaceServiceAccounts	Concede permissão para listar contas de serviço em um espaço de trabalho	Leitura	workspace*		
ListWorkspaces	Concede permissão para listar espaços de trabalho	Leitura			
TagResource	Concede permissão para adicionar etiquetas ou atualizar valores de etiquetas de um espaço de trabalho	Tags	workspace*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para remover etiquetas de um espaço de trabalho	Tags	workspace*		
				aws:TagKeys	
UpdatePermissions	Concede permissão para modificar as permissões em um espaço de trabalho	Permissions management	workspace*		
UpdateWorkspace	Concede permissão para modificar um espaço de trabalho	Gravar	workspace*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetManagedPrefixListEntries iam:CreateServiceLinkedRole
UpdateWorkspaceAuthentication	Concede permissão para modificar os provedores de autenticação em um espaço de trabalho	Gravar	workspace*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateWorkspaceConfiguration	Concede permissão para atualizar a string de configuração de um determinado espaço de trabalho	Gravar	workspace *		

Tipos de recursos definidos pelo Amazon Managed Grafana

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
workspace	`arn:${Partition}:grafana:${Region}:${Account}:/workspaces/${ResourceId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o Amazon Managed Grafana

O Amazon Managed Grafana define as chaves de condição a seguir que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por ações com base na presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por ações com base nos pares de chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso por ações com base na presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o Amazon Managed Service for Prometheus

O Amazon Managed Service for Prometheus (prefixo de serviço: `aps`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos de serviço para uso em políticas de IAM permissão.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Managed Service para Prometheus
- Tipos de recursos definidos pelo Amazon Managed Service for Prometheus
- Chaves de condição para o Amazon Managed Service for Prometheus

Ações definidas pelo Amazon Managed Service para Prometheus

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando

usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAlertManagerAlerts	Concede permissão para criar alertas	Gravar	workspace*		
				aws:ResourceTag/${TagKey}	
CreateAlertManagerDefinition	Concede permissão para criar uma definição de gerenciador de alertas	Gravar	workspace*		
				aws:ResourceTag/${TagKey}	
CreateLoggingConfiguration	Concede permissão para criar uma configuração de log	Gravar	workspace*		
				aws:ResourceTag/${TagKey}	
CreateQueryLoggingConfiguration	Concede permissão para criar uma configuração de registro de consultas	Gravar	workspace*		
				aws:ResourceTag/${TagKey}	
CreateRuleGroupsNamespace	Concede permissão para criar um namespace de grupos de regras	Gravar	rulegroupsnamespace*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateScraper	Concede permissão para criar um descarte	Gravar	cluster*		aps:TagResource ec2:DescribeSecurityGroups ec2:DescribeSubnets eks:DescribeCluster iam:CreateServiceLinkedRole
			workspace*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateWorkspace	Concede permissão para criar um Workspace	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAlertManagerDefinition	Concede permissão para excluir uma definição de gerenciador de alertas	Gravar	workspace*		
				aws:ResourceTag/${TagKey}	
DeleteAlertManagerSilence	Concede permissão para excluir um silêncio	Gravar	workspace*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteLoggingConfiguration	Concede permissão para excluir uma configuração de log	Gravar	workspace*		
				aws:ResourceTag/${TagKey}	
DeleteQueryLoggingConfiguration	Concede permissão para excluir uma configuração de registro de consultas	Gravar	workspace*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	Concede permissão para excluir a política de recursos do espaço de trabalho	Gravar	workspace*		
				aws:ResourceTag/${TagKey}	
DeleteRuleGroupsNamespace	Concede permissão para excluir um namespace de grupos de regras	Gravar	rulegroupsnamespace*		
				aws:ResourceTag/${TagKey}	
DeleteScraper	Concede permissão para excluir um descarte	Gravar	scraper*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteWorkspace	Concede permissão para excluir um Workspace	Gravar	workspace*		
				aws:ResourceTag/${TagKey}	
DescribeAlertManagerDefinition	Concede permissão para descrever uma definição de gerenciador de alertas	Leitura	workspace*		
				aws:ResourceTag/${TagKey}	
DescribeLoggingConfiguration	Concede permissão para descrever uma configuração de log	Leitura	workspace*		
				aws:ResourceTag/${TagKey}	
DescribeQueryLoggingConfiguration	Concede permissão para descrever uma configuração de registro de consultas	Leitura	workspace*		
				aws:ResourceTag/${TagKey}	
DescribeResourcePolicy	Concede permissão para descrever a política de recursos do espaço de trabalho	Leitura	workspace*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeRuleGroupsNamespace	Concede permissão para descrever um namespace de grupos de regras	Leitura	rulegroupsnamespace*		
				aws:ResourceTag/${TagKey}	
DescribeScraper	Concede permissão para descrever um descarte		scraper*		
				aws:ResourceTag/${TagKey}	
DescribeWorkspace	Concede permissão para descrever um Workspace		workspace*		
				aws:ResourceTag/${TagKey}	
DescribeWorkspaceConfiguration	Concede permissão para descrever a configuração do espaço de trabalho		workspace*		
				aws:ResourceTag/${TagKey}	
GetAlertManagerSilence	Concede permissão para obter um silêncio		workspace*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAlertManagerStatus	Concede permissão para obter o status atual de um alertmanager	Leitura	workspace*		
				aws:ResourceTag/${TagKey}	
GetDefaultScraperConfiguration	Concede permissão para obter uma configuração de descarte padrão	Leitura			
GetLabels	Concede permissão para recuperar rótulos de espaço de trabalho AMP	Read	workspace*		
				aws:ResourceTag/${TagKey}	
GetMetricMetadata	Concede permissão para recuperar os metadados para métricas do espaço de trabalho AMP	Read	workspace*		
				aws:ResourceTag/${TagKey}	
GetSeries	Concede permissão para recuperar dados de séries temporais do espaço de trabalho AMP	Leitura	workspace*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAlertManagerAlertGroups	Concede permissão para listar grupos	Leitura	workspace*		
				aws:ResourceTag/${TagKey}	
ListAlertManagerAlerts	Concede permissão para listar alertas	Leitura	workspace*		
				aws:ResourceTag/${TagKey}	
ListAlertManagerReceivers	Concede permissão para listar receptores	Leitura	workspace*		
				aws:ResourceTag/${TagKey}	
ListAlertManagerSilences	Concede permissão para listar silêncios	Leitura	workspace*		
				aws:ResourceTag/${TagKey}	
ListAlerts	Concede permissão para listar alertas ativos	Leitura	workspace*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListRuleGroupsNamespaces	Concede permissão para listar namespaces de grupos de regras	Lista	workspace*		
				aws:ResourceTag/${TagKey}	
ListRules	Concede permissão para listar regras de alerta e gravação	Leitura	workspace*		
				aws:ResourceTag/${TagKey}	
ListScrapers	Concede permissão para listar descartes	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso AMP	Leitura	rulegroupsnamespace		
			scraper		
			workspace		
				aws:TagKeys aws:RequestTag/${TagKey}	
ListWorkspaces	Concede permissão para listar espaços de trabalho	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutAlertManagerDefinition	Concede permissão para atualizar uma definição de gerenciador de alertas	Gravar	workspace*		
				aws:ResourceTag/${TagKey}	
PutAlertManagerSilences	Concede permissão para criar ou atualizar um silêncio	Gravar	workspace*		
				aws:ResourceTag/${TagKey}	
PutResourcePolicy	Concede permissão para criar e atualizar a política de recursos do espaço de trabalho	Gravar	workspace*		
				aws:ResourceTag/${TagKey}	
PutRuleGroupsNamespace	Concede permissão para atualizar um namespace de grupos de regras	Gravar	rulegroupsnamespace*		
				aws:ResourceTag/${TagKey}	
QueryMetrics	Concede permissão para executar uma consulta em métricas de espaço de trabalho AMP	Read	workspace*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
RemoteWrite	Concede permissão para executar uma operação de gravação remota para iniciar a transmissão de métricas para o espaço de trabalho AMP	Gravar	workspace*		
				aws:ResourceTag/${TagKey}	
TagResource	Concede permissão para etiquetar um recurso AMP	Tags	rulegroupsnamespace		
			scraper		
			workspace		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para desetiquetar um recurso AMP	Tags	rulegroupsnamespace		
			scraper		
			workspace		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
UpdateLoggingConfiguration	Concede permissão para atualizar uma configuração de log	Gravar	workspace*		
				aws:ResourceTag/${TagKey}	
UpdateQueryLoggingConfiguration	Concede permissão para atualizar uma configuração de registro de consultas	Gravar	workspace*		
				aws:ResourceTag/${TagKey}	
UpdateScraper	Concede permissão para atualizar um raspador	Gravar	scraper*		aps:CreateScraper aps:TagResource
			workspace		
				aws:ResourceTag/${TagKey}	
UpdateWorkspaceAlias	Concede permissão para modificar o alias do espaço de trabalho AMP existente	Gravar	workspace*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
UpdateWorkspaceConfiguration	Concede permissão para atualizar a configuração do espaço de trabalho	Gravar	workspace *		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pelo Amazon Managed Service for Prometheus

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
workspace	`arn:${Partition}:aps:${Region}:${Account}:workspace/${WorkspaceId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição para o Amazon Managed Service for Prometheus

O Amazon Managed Services for Prometheus define as seguintes chaves de condição que podem ser usadas no elemento `Condition`de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base nas etiquetas transmitidas na solicitação	String

Chaves de condição	Descrição	Type
aws:ResourceTag/${TagKey}	Filtra as ações com base nas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra ações com base nas chaves da etiqueta transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Managed Streaming for Apache Kafka

O Amazon Managed Streaming for Apache Kafka (prefixo do serviço: `kafka`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Managed Streaming for Apache Kafka
- Tipos de recursos definidos pelo Amazon Managed Streaming for Apache Kafka
- Chaves de condição do Amazon Managed Streaming for Apache Kafka

Ações definidas pelo Amazon Managed Streaming for Apache Kafka

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchAssociateScramSecret	Concede permissão para associar um ou mais Scram Secrets a um cluster do Amazon MSK	Write	cluster*		kms:CreateGrant kms:RetireGrant
BatchDisassociateScramSecret	Concede permissão para desassociar um ou mais Scram Secrets de um cluster do Amazon MSK	Write	cluster*		kms:RetireGrant
CreateCluster	Concede permissão para criar um cluster MSK	Gravar	cluster*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					kms:CreateGrant kms:DescribeKey
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateClusterV2	Concede permissão para criar um cluster MSK	Write	cluster*		ec2:CreateTags ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs iam:AttachRolePolicy

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					iam:CreateServiceLinkedRole iam:PutRolePolicy kms:CreateGrant kms:DescribeKey
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfiguration	Concede permissão para criar uma configuração MSK	Gravar	configuration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateReplicator	Concede permissão para criar um replicador do MSK	Gravar	replicator*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PassRole iam:PutRolePolicy kafka:DescribeClusterV2 kafka:GetBootstrapBrokers

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateVpcConnection	Concede permissão para criar uma conexão MSK VPC	Gravar	cluster*		ec2:CreateTags ec2:CreateVpcEndpoint ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs iam:AttachRolePolicy iam:CreateServiceLinkedRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					iam:PutRolePolicy
			vpc-connection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCluster	Concede permissão para excluir um cluster MSK	Gravar	cluster*		ec2:DeleteVpcEndpoints ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints
DeleteClusterPolicy	Concede permissão para excluir uma política baseada em recursos de cluster	Gravar	cluster*		
DeleteConfiguration	Concede permissão para excluir a configuração especificada do MSK	Gravar	configuration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteReplicator	Concede permissão para excluir um replicador do MSK	Gravar	replicator*		
DeleteVpcConnection	Concede permissão para excluir uma conexão MSK VPC	Gravar	vpc-connection*		ec2:DeleteVpcEndpoints ec2:DescribeVpcEndpoints
DescribeCluster	Concede permissão para descrever um cluster MSK	Read	cluster*		
DescribeClusterOperation	Concede permissão para descrever a operação de cluster especificada pelo ARN fornecido	Leitura			
DescribeClusterOperationV2	Concede permissão para descrever a operação de cluster especificada pelo ARN fornecido	Leitura			
DescribeClusterV2	Concede permissão para descrever um cluster MSK	Leitura	cluster*		
DescribeConfiguration	Concede permissão para descrever uma configuração MSK	Read	configuration*		
DescribeConfigurationRevision	Concede permissão para descrever uma revisão de configuração MSK	Leitura	configuration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeReplicator	Concede permissão para descrever um replicador do MSK	Leitura	replicator*		
DescribeVpcConnection	Concede permissão para descrever uma conexão MSK VPC	Leitura	vpc-connection*		
GetBootstrapBrokers	Concede permissão para obter detalhes de conexão para os corretores em um cluster MSK	Leitura			
GetClusterPolicy	Concede permissão para descrever uma política baseada em recursos de cluster	Leitura	cluster*		
GetCompatibleKafkaVersions	Concede permissão para obter uma lista das versões do Apache Kafka para as quais você pode atualizar um cluster MSK	Lista			
ListClientVpcConnections	Concede permissão para listar todas as conexões MSK VPC criadas para um cluster	Lista	cluster*		
ListClusterOperations	Concede permissão para retornar uma lista de todas as operações que foram executadas no cluster MSK especificado	Lista	cluster*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListClusterOperationsV2	Concede permissão para retornar uma lista de todas as operações que foram executadas no cluster MSK especificado	List	cluster*		
ListClusters	Concede permissão para listar todos os clusters MSK nesta conta	Lista			
ListClustersV2	Concede permissão para listar todos os clusters MSK nesta conta	List			
ListConfigurationRevisions	Concede permissão para listar todas as revisões para uma configuração MSK nesta conta	List	configuration*		
ListConfigurations	Concede permissão para listar todas as configurações do MSK nesta conta	List			
ListKafkaVersions	Concede permissão para listar todas as versões do Apache Kafka suportadas pelo Amazon MSK	List			
ListNodes	Concede permissão para listar agentes em um cluster MSK	Lista	cluster*		
ListReplicators	Concede permissão para listar todos os replicadores do MSK nesta conta	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListScramSecrets	Concede permissão para listar os Scram Secrets associados a um cluster do Amazon MSK	List	cluster*		
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso MSK	Leitura	cluster*		
ListVpcConnections	Concede permissão para listar todas as conexões MSK VPC usadas por esta conta	Lista			
PutClusterPolicy	Concede permissão para criar ou atualizar a política baseada em recursos para um cluster	Gravar	cluster*		
RebootBroker	Concede permissão para reiniciar o agente	Gravar	cluster*		
RejectClientVpcConnection	Concede permissão para rejeitar uma conexão MSK VPC	Gravar	cluster*		
			vpc-connection*		
TagResource	Concede permissão para marcar um recurso MSK	Marcação	cluster		
			vpc-connection		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover etiquetas de um recurso MSK	Marcação	cluster		
			vpc-connection		
				aws:TagKeys	
UpdateBrokerCount	Concede permissão para atualizar o número de agentes do cluster MSK	Write	cluster*		
UpdateBrokerStorage	Concede permissão para atualizar o tamanho do armazenamento dos agentes do cluster MSK	Write	cluster*		
UpdateBrokerType	Concede permissão para atualizar o tipo de agente de um cluster do Amazon MSK	Write	cluster*		
UpdateClusterConfiguration	Concede permissão para atualizar a configuração do cluster do MSK	Write	cluster*		
			configuration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateClusterKafkaVersion	Concede permissão para atualizar o cluster do MSK para a versão especificada do Apache Kafka	Write	cluster*		
UpdateConfiguration	Concede permissão para criar uma nova revisão da configuração do MSK	Gravar	configuration*		
UpdateConnectivity	Concede permissão para atualizar as configurações de conectividade para o cluster do MSK	Gravar	cluster*		ec2:DescribeRouteTables ec2:DescribeSubnets
				kafka:publicAccessEnabled	
UpdateMonitoring	Concede permissão para atualizar as configurações de monitoramento para o cluster do MSK	Gravar	cluster*		
UpdateReplicationInfo	Concede permissão para atualizar as informações de replicação do replicador do MSK	Gravar	replicator*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateSecurity	Concede permissão para atualizar as configurações de segurança para o cluster do MSK	Gravar	cluster*		kms:RetireGrant
UpdateStorage	Concede permissão para atualizar o armazenamento do EBS (tamanho ou throughput provisionado) associado aos agentes do MSK ou para definir o modo de armazenamento do cluster como TIERED	Gravar	cluster*		

Tipos de recursos definidos pelo Amazon Managed Streaming for Apache Kafka

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
cluster	`arn:${Partition}:kafka:${Region}:${Account}:cluster/${ClusterName}/${Uuid}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
configuration	`arn:${Partition}:kafka:${Region}:${Account}:configuration/${ConfigurationName}/${Uuid}`	
vpc-connection	`arn:${Partition}:kafka:${Region}:${VpcOwnerAccount}:vpc-connection/${ClusterOwnerAccount}/${ClusterName}/${Uuid}`	aws:ResourceTag/${TagKey}
replicator	`arn:${Partition}:kafka:${Region}:${Account}:replicator/${ReplicatorName}/${Uuid}`	aws:ResourceTag/${TagKey}
topic	`arn:${Partition}:kafka:${Region}:${Account}:topic/${ClusterName}/${ClusterUuid}/${TopicName}`	
group	`arn:${Partition}:kafka:${Region}:${Account}:group/${ClusterName}/${ClusterUuid}/${GroupName}`	
transactional-id	`arn:${Partition}:kafka:${Region}:${Account}:transactional-id/${ClusterName}/${ClusterUuid}/${TransactionalId}`	

Chaves de condição do Amazon Managed Streaming for Apache Kafka

O Amazon Managed Streaming for Apache Kafka define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString
kafka:publicAccessEnabled	Filtra o acesso pela presença de acesso público habilitado na solicitação	Bool

Ações, recursos e chaves de condição do Amazon Managed Streaming for Kafka Connect

O Amazon Managed Streaming for Kafka Connect (prefixo do serviço: `kafkaconnect`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Managed Streaming for Kafka Connect
- Tipos de recursos definidos pelo Amazon Managed Streaming for Kafka Connect
- Chaves de condição para o Amazon Managed Streaming for Kafka Connect

Ações definidas pelo Amazon Managed Streaming for Kafka Connect

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateConnector	Concede permissão para criar uma configuração do conector MSK Connect	Gravar			ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs firehose:TagDeliveryStream iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PassRole iam:PutRolePolicy

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					logs:CreateLogDelivery logs:DescribeLogGroups logs:DescribeResourcePolicies logs:GetLogDelivery logs:ListLogDeliveries logs:PutResourcePolicy s3:GetBucketPolicy s3:PutBucketPolicy
CreateCustomPlugin	Concede permissão para criar um plugin personalizado MSK Connect	Gravar			s3:GetObject

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateWorkerConfiguration	Concede permissão para criar uma configuração de operador do MSK Connect	Gravar			
DeleteConnector	Concede permissão para excluir uma configuração do conector MSK Connect	Gravar	connector*		logs:DeleteLogDelivery logs:ListLogDeliveries
DeleteCustomPlugin	Concede permissão para excluir um plugin personalizado MSK Connect	Gravar	custom plugin*		
DeleteWorkerConfiguration	Concede permissão para excluir uma configuração do trabalhador do MSK Connect	Gravar	worker configuration*		
DescribeConnector	Concede permissão para descrever uma configuração do conector MSK Connect	Leitura	connector*		
DescribeConnectorOperation	Concede permissão para descrever uma operação do conector MSK Connect	Leitura	connector operation*		
DescribeCustomPlugin	Concede permissão para descrever um plugin personalizado MSK Connect	Leitura	custom plugin*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeWorkerConfiguration	Concede permissão para descrever uma configuração do operador do MSK Connect	Leitura	worker configuration*		
ListConnectorOperations	Concede permissão para listar todas as operações de um determinado conector MSK Connect	Leitura	connector*		
ListConnectors	Concede permissão para listar todos os conectores do MSK Connect nesta conta	Leitura			
ListCustomPlugins	Concede permissão para listar todos os plugins personalizados do MSK Connect nesta conta	Leitura			
ListTagsForResource	Concede permissão para listar as tags de um recurso do MSK Connect	Leitura	connector	aws:ResourceTag/${TagKey}	
			custom plugin	aws:ResourceTag/${TagKey}	
			worker configuration	aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListWorkerConfigurations	Concede permissão para listar todas as configurações dos operadores do MSK Connect nesta conta	Leitura			
TagResource	Concede permissão para marcar um recurso do MSK Connect	Tags	connector	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			custom plugin	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			worker configuration	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover as tags de um recurso do MSK Connect	Tags	connector	aws:TagKeys	
			custom plugin	aws:TagKeys	
			worker configuration	aws:TagKeys	
				aws:TagKeys	
UpdateConnector	Concede permissão para atualizar uma configuração do conector MSK Connect	Gravar	connector *		

Tipos de recursos definidos pelo Amazon Managed Streaming for Kafka Connect

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição para o Amazon Managed Streaming for Kafka Connect

O Amazon Managed Streaming para Kafka Connect define as chaves de condição a seguir que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o Amazon Managed Workflows for Apache Airflow

O Amazon Managed Workflows for Apache Airflow (prefixo de serviço: `airflow`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos de serviço para uso em IAM políticas de permissão.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Managed Workflows for Apache Airflow
- Tipos de recursos definidos pelo Amazon Managed Workflows for Apache Airflow
- Chaves de condição para o Amazon Managed Workflows for Apache Airflow

Ações definidas pelo Amazon Managed Workflows for Apache Airflow

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando

usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateCliToken	Concede permissão para criar um token de curta duração que permite a um usuário invocar a CLI do Airflow por meio de um endpoint no servidor da Web Apache Airflow	Write	environment*		
CreateEnvironment	Concede permissão para criar um ambiente do Amazon MWAA	Write	environment*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebLoginToken	Concede permissão para criar um token de curta duração que permite ao usuário fazer login na IU da Web do Apache Airflow	Write	rbac-role*		
DeleteEnvironment	Concede permissão para excluir um ambiente do Amazon MWAA	Write	environment*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
GetEnvironment	Concede permissão para visualizar detalhes sobre um ambiente do Amazon MWAA	Leitura	environment*		
				aws:ResourceTag/${TagKey}	
InvokeRestApi	Concede permissão para invocar a API REST do Airflow por meio de um endpoint no servidor da Web Apache Airflow	Gravar	rbac-role*		
ListEnvironments	Concede permissão para listar os ambientes do Amazon MWAA em sua conta	List			
ListTagsForResource	Concede permissão para etiquetas de listas para um ambiente do Amazon MWAA	Read	environment		
				aws:ResourceTag/${TagKey}	
PublishMetrics	Concede permissão para publicar métricas para um ambiente do Amazon MWAA	Write	environment*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para marcar um ambiente do Amazon MWAA	Marcação	environment		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permissão para desmarcar um ambiente do Amazon MWAA	Marcação	environment		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateEnvironment	Concede permissão para modificar um ambiente do Amazon MWAA	Write	environment*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pelo Amazon Managed Workflows for Apache Airflow

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
environment	`arn:${Partition}:airflow:${Region}:${Account}:environment/${EnvironmentName}`	
rbac-role	`arn:${Partition}:airflow:${Region}:${Account}:role/${EnvironmentName}/${RoleName}`	

Chaves de condição para o Amazon Managed Workflows for Apache Airflow

O Amazon Managed Workflows for Apache Airflow define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma IAM política. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS Marketplace

AWS Marketplace (prefixo do serviço:`aws-marketplace`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Marketplace
- Tipos de recursos definidos pelo AWS Marketplace
- Chaves de condição do AWS Marketplace

Ações definidas pelo AWS Marketplace

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o

nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptAgreementApprovalRequest	Concede permissão aos usuários para aprovar uma solicitação de assinatura	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	recebida (para provedores que fornecem produtos que exigem verificação de assinatura)				
AcceptAgreementRequest	Concede aos usuários permissão para aceitar solicitações de contrato. Essa ação não se aplica a compras no Marketplace	Gravar			
CancelAgreement	Concede aos usuários permissão para cancelar contratos. Essa ação não se aplica a compras no Marketplace	Gravar			
CancelAgreementRequest	Concede permissão aos usuários para cancelar solicitações de assinatura pendentes para produtos que exigem verificação de assinatura	Gravar			
CreateAgreementRequest	Concede permissão aos usuários para criar uma solicitação de contrato. Essa ação não se aplica a compras no Marketplace	Gravar			
DescribeAgreement	Concede permissão aos usuários para descrever os metadados sobre o contrato	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAgreementApprovalRequest	Concede permissão aos usuários para visualizar os detalhes de suas solicitações de assinatura recebidas (para provedores que fornecem produtos que exigem verificação de assinatura)	Leitura			
GetAgreementEntitlements	Concede permissão aos usuários para visualizar os direitos associados a um contrato	Leitura			
GetAgreementRequest	Concede permissão aos usuários para visualizar os detalhes de suas solicitações de assinatura para produtos de dados que exigem verificação de assinatura	Leitura			
GetAgreementTerms	Concede permissão aos usuários para obter uma lista de termos para um contrato	Lista			
ListAgreementApprovalRequests	Concede permissão aos usuários para listar suas solicitações de assinatura recebidas (para provedores que fornecem produtos que exigem verificação de assinatura)	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAgreementCharges	Concede permissão aos usuários para visualizar as cobranças associadas aos seus contratos	Lista			
ListAgreementRequests	Concede permissão aos usuários para listar suas solicitações de assinatura pendentes para produtos que exigem verificação de assinatura	Lista			
ListEntitlementDetails	Concede permissão aos usuários para visualizar detalhes dos direitos associados a um contrato. Essa ação não se aplica a compras no Marketplace	Leitura			
RejectAgreementApprovalRequest	Concede permissão aos usuários para recusar solicitações de assinatura recebidas (para provedores que fornecem produtos que exigem verificação de assinatura)	Gravar			
SearchAgreements	Concede permissão aos usuários para pesquisar seus contratos	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
Subscribe	Concede permissão aos usuários para assinar AWS Marketplace produtos. Inclui a capacidade de enviar uma solicitação de assinatura para produtos que exigem verificação de assinatura. Inclui a capacidade de habilitar a renovação automática de uma assinatura existente	Gravar			
Unsubscribe	Concede permissão aos usuários para remover assinaturas de produtos. AWS Marketplace Inclui a capacidade de desabilitar a renovação automática de uma assinatura existente	Gravar			
UpdateAgreementApprovalRequest	Concede permissão aos usuários para fazer alterações em uma solicitação de assinatura recebida, incluindo a capacidade de excluir as informações do potencial assinante (para provedores que fornecem produtos que exigem verificação de assinatura)	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdatePurchaseOrders	Concede permissão aos usuários para atualizar os pedidos de compra para cobranças associadas a seus contratos	Gravar			
ViewSubscriptions	Concede permissão aos usuários para ver as assinaturas de suas contas	Lista			

Tipos de recursos definidos pelo AWS Marketplace

AWS Marketplace não suporta a especificação de um ARN de recurso no elemento de uma `Resource` declaração de política do IAM. Para conceder acesso ao AWS Marketplace, especifique `"Resource": "*"` na política.

Chaves de condição do AWS Marketplace

AWS Marketplace define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws-marketplace:AgreementType	Filtra o acesso por tipo do contrato	ArrayOfString

Chaves de condição	Descrição	Tipo
aws-marketplace:PartyType	Filtra o acesso pela parte do contrato	String
aws-marketplace:ProductId	Filtra o acesso por ID de produto AWS Marketplace RedHat OpenShift e produtos Bedrock. Nota: O uso dessa chave de condição não restringirá o acesso aos produtos em AWS Marketplace	ArrayOfString

Ações, recursos e chaves de condição do AWS Marketplace Catalog

AWS Marketplace O catálogo (prefixo do serviço:`aws-marketplace`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Marketplace Catalog
- Tipos de recursos definidos pelo AWS Marketplace Catalog
- Chaves de condição do AWS Marketplace Catalog

Ações definidas pelo AWS Marketplace Catalog

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelChangeSet	Concede permissão para cancelar um conjunto de alterações em execução	Gravar	ChangeSet*		
DeleteResourcePolicy	Concede permissão para excluir a política de recursos de uma entidade existente	Gerenciamento de permissões	Entity*		
DescribeAssessment	Concede permissão para retornar os detalhes de uma avaliação existente	Leitura			
DescribeChangeSet	Concede permissão para retornar os detalhes de um conjunto de alterações existente	Leitura	ChangeSet*		
DescribeEntity	Concede permissão para retornar os detalhes de uma entidade existente	Leitura	Entity*		
GetResourcePolicy	Concede permissão para obter a política de recursos de uma entidade existente	Leitura	Entity*		
ListAssessments	Concede permissão para listar as avaliações existentes	Lista			
ListChangeSets	Concede permissão para listar conjuntos de mudanças existentes	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListEntities	Concede permissão para listar as entidades existentes	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de uma entidade existente ou um conjunto de alterações	Leitura	ChangeSet		
			Entity		
PutResourcePolicy	Concede permissão para anexar uma política de recursos a uma entidade existente	Gerenciamento de permissões	Entity*		
StartChangeSet	Concede permissão para solicitar um novo conjunto de alterações (Observação: as permissões em nível de recurso para essa ação e as chaves de contexto de condição para essa ação só são suportadas quando usadas com a API do Catalog e não são suportadas quando usadas com AWS Marketplace o Management Portal)	Gravar	Entity*		
				catalog:ChangeType aws-marketplace:Intent aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Concede permissão para etiquetar uma entidade existente ou um conjunto de alterações	Tags	ChangeSet		
			Entity		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover etiquetas de uma entidade existente ou um de conjunto de alterações	Tags	ChangeSet		
			Entity		
				aws:TagKeys	

Tipos de recursos definidos pelo AWS Marketplace Catalog

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
Entity	`arn:${Partition}:aws-marketplace:${Region}:${Account}:${Catalog}/${EntityType}/${ResourceId}`	aws:ResourceTag/${TagKey} catalog:ChangeType

Tipos de recursos	ARN	Chaves de condição
ChangeSet	`arn:${Partition}:aws-marketplace:${Region}:${Account}:${Catalog}/ChangeSet/${ResourceId}`	aws:ResourceTag/${TagKey} catalog:ChangeType

Chaves de condição do AWS Marketplace Catalog

AWS Marketplace O catálogo define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws-marketplace:Intent	Filtra o acesso pelo parâmetro Intent na solicitação StartChangeSet	String
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString
catalog:ChangeType	Filtra o acesso pelo tipo de alteração na StartChangeSet solicitação	String

Ações, recursos e chaves de condição do AWS Marketplace Commerce Analytics Service

AWS Marketplace O Commerce Analytics Service (prefixo do serviço:`marketplacecommerceanalytics`) fornece os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.

Tópicos

- Ações definidas pelo AWS Marketplace Commerce Analytics Service
- Tipos de recursos definidos pelo AWS Marketplace Commerce Analytics Service
- Chaves de condição para o AWS Marketplace Commerce Analytics Service

Ações definidas pelo AWS Marketplace Commerce Analytics Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GenerateDataSet	Solicite um conjunto de dados a ser publicado no bucket do Amazon S3.	Write			
StartSupportDataExport	Solicite um conjunto de dados de suporte a ser publicado no bucket do Amazon S3.	Write			

Tipos de recursos definidos pelo AWS Marketplace Commerce Analytics Service

AWS Marketplace O Commerce Analytics Service não suporta a especificação de um ARN de recurso `Resource` no elemento de uma declaração de política do IAM. Para permitir o acesso ao AWS Marketplace Commerce Analytics Service, especifique `"Resource": "*"` na política.

Chaves de condição para o AWS Marketplace Commerce Analytics Service

O CAS não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento de instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do Serviço de Implantação da AWS Marketplace

AWS Marketplace O Serviço de Implantação (prefixo do serviço:`aws-marketplace`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Serviço de Implantação da AWS Marketplace
- Tipos de recursos definidos pelo Serviço de Implantação da AWS Marketplace
- Chaves de condição do Serviço de Implantação da AWS Marketplace

Ações definidas pelo Serviço de Implantação da AWS Marketplace

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar tags para um recurso de parâmetro de implantação	Leitura	DeploymentParameter		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
PutDeploymentParameter	Concede permissão para criar ou atualizar um recurso de parâmetro de implantação	Gravar	DeploymentParameter*	aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	aws-marketplace:TagResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para atribuir tags a um recurso de parâmetro de implantação	Tags	DeploymentParameter*	aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover tags de um recurso de parâmetro de implantação	Tags	DeploymentParameter*	aws:ResourceTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:TagKeys	

Tipos de recursos definidos pelo Serviço de Implantação da AWS Marketplace

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
DeploymentParameter	`arn:${Partition}:aws-marketplace:${Region}:${Account}:DeploymentParameter:catalogs/${CatalogName}/products/${ProductId}/${ResourceId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Chaves de condição do Serviço de Implantação da AWS Marketplace

AWS Marketplace O Serviço de Implantação define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar

ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves de etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Marketplace Discovery

AWS Marketplace O Discovery (prefixo do serviço:`aws-marketplace`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Marketplace Discovery
- Tipos de recursos definidos pelo AWS Marketplace Discovery
- Chaves de condição do AWS Marketplace Discovery

Ações definidas pelo AWS Marketplace Discovery

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListPrivateListings	Concede permissão aos usuários para listar suas ofertas privadas	Lista			

Tipos de recursos definidos pelo AWS Marketplace Discovery

AWS Marketplace O Discovery não suporta a especificação de um ARN de recurso `Resource` no elemento de uma declaração de política do IAM. Para permitir acesso ao AWS Marketplace Discovery, especifique `"Resource": "*"` na política.

Chaves de condição do AWS Marketplace Discovery

O Marketplace Discovery não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` de declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Marketplace Entitlement Service

AWS Marketplace O Entitlement Service (prefixo do serviço:`aws-marketplace`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Marketplace Entitlement Service
- Tipos de recursos definidos pelo AWS Marketplace Entitlement Service
- Chaves de condição do AWS Marketplace Entitlement Service

Ações definidas pelo AWS Marketplace Entitlement Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de

recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetEntitlements	Concede permissão para recuperar valores de autorização para um determinado produto. Os resultados podem ser filtrados com base no identificador do cliente ou nas dimensões do produto	Read			

Tipos de recursos definidos pelo AWS Marketplace Entitlement Service

AWS Marketplace O Entitlement Service não suporta a especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para conceder acesso ao AWS Marketplace Entitlement Service, especifique `"Resource": "*"` na política.

Chaves de condição do AWS Marketplace Entitlement Service

A autorização do Marketplace não tem chaves de contexto específicas ao serviço que possam ser usadas no elemento `Condition` de instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Marketplace Image Building Service

AWS Marketplace O Image Building Service (prefixo do serviço:`aws-marketplace`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Marketplace Image Building Service
- Tipos de recursos definidos pelo AWS Marketplace Image Building Service
- Chaves de condição do AWS Marketplace Image Building Service

Ações definidas pelo AWS Marketplace Image Building Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa

ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeBuilds [somente permissão]	Descreve criações de imagens identificadas por um ID de criação	Read			
ListBuilds [somente permissão]	Lista criações de imagens.	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartBuild [somente permissão]	Inicia uma criação de imagem	Write			

Tipos de recursos definidos pelo AWS Marketplace Image Building Service

AWS Marketplace O Image Building Service não suporta a especificação de um ARN de recurso no elemento de uma `Resource` declaração de política do IAM. Para conceder acesso ao AWS Marketplace Image Building Service, especifique `"Resource": "*"` na política.

Chaves de condição do AWS Marketplace Image Building Service

A criação de imagens do Marketplace não tem chaves de contexto específicas ao serviço que possam ser usadas no elemento `Condition` de instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Marketplace Management Portal

AWS Marketplace O Portal de Gerenciamento (prefixo do serviço:`aws-marketplace-management`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Marketplace Management Portal
- Tipos de recursos definidos pelo AWS Marketplace Management Portal
- Chaves de condição do AWS Marketplace Management Portal

Ações definidas pelo AWS Marketplace Management Portal

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de

recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAdditionalSellerNotificationRecipients [somente permissão]	Concede permissão para visualizar destinatários adicionais de notificação do vendedor	Leitura			
GetBankAccountVerificationDetails [somente permissão]	Concede permissão para visualizar o status de verificação da conta bancária	Leitura			
GetSecondaryUserVerificationDetails [somente permissão]	Concede permissão para visualizar o status de verificação da conta do usuário secundário	Leitura			
GetSellerVerificationDetails	Concede permissão para visualizar o status de verificação da conta	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
[somente permissão]					
PutAdditionalSellerNotificationRecipients [somente permissão]	Concede permissão para atualizar destinatários adicionais de notificação do vendedor	Gravar			
PutBankAccountVerificationDetails [somente permissão]	Concede permissão para atualizar o status de verificação da conta bancária	Gravar			
PutSecondaryUserVerificationDetails [somente permissão]	Concede permissão para atualizar o status de verificação da conta do usuário secundário	Gravar			
PutSellerVerificationDetails [somente permissão]	Concede permissão para atualizar o status de verificação da conta	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
uploadFiles [somente permissão]	Permite acesso à página de upload de arquivos dentro do Portal AWS Marketplace de Gerenciamento	Gravar			
viewMarketing [somente permissão]	Permite o acesso à página de Marketing dentro do Portal AWS Marketplace de Gerenciamento	Lista			
viewReports [somente permissão]	Permite acesso à página de Relatórios dentro do Portal AWS Marketplace de Gerenciamento	Lista			
viewSettings [somente permissão]	Permite o acesso à página de Configurações dentro do Portal AWS Marketplace de Gerenciamento	Lista			
viewSupport [somente permissão]	Permite acesso à página de elegibilidade do Customer Support dentro do Portal AWS Marketplace de Gerenciamento	Lista			

Tipos de recursos definidos pelo AWS Marketplace Management Portal

AWS Marketplace O Portal de Gerenciamento não suporta a especificação de um ARN de recurso no elemento de uma `Resource` declaração de política do IAM. Para conceder acesso ao AWS Marketplace Management Portal, especifique `"Resource": "*"` na política.

Chaves de condição do AWS Marketplace Management Portal

O Portal do Marketplace não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Marketplace Metering Service

AWS Marketplace O Metering Service (prefixo do serviço:`aws-marketplace`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Marketplace Metering Service
- Tipos de recursos definidos pelo AWS Marketplace Metering Service
- Chaves de condição do AWS Marketplace Metering Service

Ações definidas pelo AWS Marketplace Metering Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o

nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchMeterUsage	Concede permissão para publicar registros de medição	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	para um conjunto de clientes para aplicações SaaS				
MeterUsage	Concede permissão para emitir registros de medição	Gravar			
RegisterUsage	Concede permissão para verificar se o cliente que está executando seu software pago está inscrito em seu produto AWS Marketplace, permitindo que você se proteja contra o uso não autorizado. Mede o uso de software por tarefa do ECS, por hora, com uso pro rata até o segundo	Gravar			
ResolveCustomer	Concede permissão para resolver um token de registro para obter um CustomerIdentifier código de produto	Gravar			

Tipos de recursos definidos pelo AWS Marketplace Metering Service

AWS Marketplace O Metering Service não suporta a especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para conceder acesso ao AWS Marketplace Metering Service, especifique `"Resource": "*"` na política.

Chaves de condição do AWS Marketplace Metering Service

A Medição do Marketplace não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de

contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Marketplace Private Marketplace

AWS Marketplace O Private Marketplace (prefixo do serviço:`aws-marketplace`) fornece os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Marketplace Private Marketplace
- Tipos de recursos definidos pelo AWS Marketplace Private Marketplace
- Chaves de condição do AWS Marketplace Private Marketplace

Ações definidas pelo AWS Marketplace Private Marketplace

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos

("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateProductsWithPrivateMarketplace [somente permissão]	Concede permissão para criar uma nova solicitação para que um produto seja associado ao Private Marketplace. Essa ação pode ser executada por qualquer conta em uma AWS organização, desde que o usuário tenha permissões	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	para fazer isso e as políticas de controle de serviços da organização permitam isso.				
CreatePrivateMarketplaceRequests [somente permissão]	Concede permissão para criar uma nova solicitação para que um produto ou produtos sejam associados ao Private Marketplace. Essa ação pode ser executada por qualquer conta em uma AWS organização, desde que o usuário tenha permissões para fazer isso e as políticas de controle de serviços da organização permitam isso.	Gravar			
DescribePrivateMarketplaceRequests [somente permissão]	Concede permissão para descrever as solicitações e os produtos associados no Private Marketplace. Essa ação pode ser executada por qualquer conta em uma AWS organização, desde que o usuário tenha permissões para fazer isso e as políticas de controle de serviços da organização permitam isso.	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateProductsFromPrivateMarketplace [somente permissão]	Concede permissão para recusar uma nova solicitação para que um produto seja associado ao Private Marketplace. Essa ação pode ser executada por qualquer conta em uma AWS organização, desde que o usuário tenha permissões para fazer isso e as políticas de controle de serviços da organização permitam isso.	Gravar			
ListPrivateMarketplaceRequests [somente permissão]	Concede permissão para obter uma lista consultável de solicitações e produtos associados no Private Marketplace. Essa ação pode ser executada por qualquer conta em uma AWS organização, desde que o usuário tenha permissões para fazer isso e as políticas de controle de serviços da organização permitam isso.	Lista			

Tipos de recursos definidos pelo AWS Marketplace Private Marketplace

AWS Marketplace O Private Marketplace não suporta a especificação de um ARN de recurso `Resource` no elemento de uma declaração de política do IAM. Para conceder acesso ao AWS Marketplace Private Marketplace, especifique `"Resource": "*"` na política.

Chaves de condição do AWS Marketplace Private Marketplace

O Private Marketplace não tem chaves de contexto específicas ao serviço que possam ser usadas no elemento `Condition` de declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Marketplace Procurement Systems Integration

AWS Marketplace O Procurement Systems Integration (prefixo do serviço:`aws-marketplace`) fornece os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Marketplace Procurement Systems Integration
- Tipos de recursos definidos pelo AWS Marketplace Procurement Systems Integration
- Chaves de condição do AWS Marketplace Procurement Systems Integration

Ações definidas pelo AWS Marketplace Procurement Systems Integration

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeProcurementSystemConfiguration	Concede permissão para descrever a configuração de integração do Sistema de Compras (por exemplo, Coupa) para a conta individual	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
[somente permissão]	ou para toda a AWS organização, se houver. Essa ação só pode ser executada pela conta principal se estiver usando uma AWS organização				
PutProcurementSystemConfiguration [somente permissão]	Concede permissão para criar ou atualizar a configuração de integração do Sistema de Compras (por exemplo, Coupa) para a conta individual ou para toda a AWS organização, se houver. Essa ação só pode ser executada pela conta principal se estiver usando uma AWS organização	Gravar			

Tipos de recursos definidos pelo AWS Marketplace Procurement Systems Integration

AWS Marketplace O Procurement Systems Integration não suporta a especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para conceder acesso ao AWS Marketplace Procurement Systems Integration, especifique `"Resource": "*"` na política.

Chaves de condição do AWS Marketplace Procurement Systems Integration

A Integração de compras do Marketplace não tem chaves de contexto específicas ao serviço que possam ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Marketplace Reporting

AWS Marketplace Os relatórios (prefixo do serviço:`aws-marketplace`) fornecem os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Marketplace Reporting
- Tipos de recursos definidos pelo AWS Marketplace Reporting
- Chaves de condição do AWS Marketplace Reporting

Ações definidas pelo AWS Marketplace Reporting

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetBuyerDashboard	Concede permissão para visualizar um painel que mostra os dados de AWS Marketplace compra do comprador	Leitura	Dashboard *		

Tipos de recursos definidos pelo AWS Marketplace Reporting

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso

também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
Dashboard	`arn:${Partition}:aws-marketplace::${Account}:${Catalog}/ReportingData/${FactTable}/Dashboard/${DashboardName}`	

Chaves de condição do AWS Marketplace Reporting

O Marketplace Reporting não tem chaves de contexto específicas do serviço que podem ser usadas no elemento `Condition` de instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Marketplace Seller Reporting

AWS Marketplace O Seller Reporting (prefixo do serviço:`aws-marketplace`) fornece os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Marketplace Seller Reporting
- Tipos de recursos definidos pelo AWS Marketplace Seller Reporting
- Chaves de condição do AWS Marketplace Seller Reporting

Ações definidas pelo AWS Marketplace Seller Reporting

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSellerDashboard	Concede permissão para exibir um painel de vendedor	Leitura	SellerDashboard*		

Tipos de recursos definidos pelo AWS Marketplace Seller Reporting

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
SellerDashboard	`arn:${Partition}:aws-marketplace::${Account}:${Catalog}/ReportingData/${FactTable}/Dashboard/${DashboardName}`	

Chaves de condição do AWS Marketplace Seller Reporting

O Marketplace Seller Reporting não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` de declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Marketplace Vendor Insights

AWS Marketplace O Vendor Insights (prefixo do serviço:`vendor-insights`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Marketplace Vendor Insights
- Tipos de recursos definidos pelo AWS Marketplace Vendor Insights
- Chaves de condição do AWS Marketplace Vendor Insights

Ações definidas pelo AWS Marketplace Vendor Insights

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar

a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ActivateSecurityProfile	Concede permissão para ativar o perfil de segurança	Gravar	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
AssociateDataSource	Concede permissão para associar o perfil de segurança a uma fonte de dados	Gravar	SecurityProfile*		vendor-insights:GetDataSource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
CreateDataSource	Concede permissão para criar uma nova fonte de dados	Gravar		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	vendor-insights:TagResource
CreateSecurityProfile	Concede permissão para criar um novo perfil de segurança	Gravar		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	vendor-insights:TagResource
DeactivateSecurityProfile	Concede permissão para desativar o perfil de segurança	Gravar	SecurityProfile*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteDataSource	Concede permissão para excluir uma fonte de dados	Gravar	DataSource*		
				aws:ResourceTag/${TagKey}	
DisassociateDataSource	Concede permissão para desassociar o perfil de segurança de uma fonte de dados	Gravar	SecurityProfile*		vendor-insights:GetDataSource
				aws:ResourceTag/${TagKey}	
GetDataSource	Concede permissão para recuperar os detalhes de uma fonte de dados existente	Leitura	DataSource*		
				aws:ResourceTag/${TagKey}	
GetEntitledSecurityProfileSnapshot	Concede permissão para retornar os detalhes de um snapshot do perfil de segurança que o solicitante está autorizado a ler	Leitura	SecurityProfile*		
GetProfileAccessTerms	Concede permissão para obter os termos de acesso de um perfil do Vendor Insights	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSecurityProfile	Concede permissão para retornar os detalhes de um perfil de segurança existente	Leitura	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
GetSecurityProfileSnapshot	Concede permissão para retornar os detalhes de um snapshot do perfil de segurança	Leitura	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
ListDataSources	Concede permissão para listar as fontes de dados existentes	Lista			
ListEntitledSecurityProfileSnapshots	Concede permissão para retornar a lista de resumo de snapshots de um perfil de segurança existente que o solicitante está autorizado a listar	Lista	SecurityProfile*		
ListEntitledSecurityProfiles	Concede permissão para listar perfis de segurança autorizados	Lista			
ListSecurityProfileSnapshots	Concede permissão para retornar a lista de resumo de snapshots de um perfil de segurança existente	Lista	SecurityProfile*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListSecurityProfiles	Concede permissão para listar perfis de segurança existentes	Lista			
ListTagsForResource	Concede permissão para listar etiquetas para recursos de insights de fornecedores	Leitura	DataSource		
			SecurityProfile		
				aws:ResourceTag/${TagKey}	
TagResource	Concede permissão para etiquetar recursos de insights de fornecedores	Tags	DataSource		
			SecurityProfile		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover etiquetas de recursos de insights de fornecedores	Tags	DataSource		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			SecurityProfile		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateDataSource	Concede permissão para atualizar uma fonte de dados existente	Gravar	DataSource*		
				aws:ResourceTag/${TagKey}	
UpdateSecurityProfile	Concede permissão para atualizar o perfil de segurança	Gravar	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
UpdateSecurityProfileSnapshotCreationConfiguration	Concede permissão para atualizar a configuração de criação de snapshot de perfil de segurança	Gravar	SecurityProfile*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateSecurityProfileSnapshotReleaseConfiguration	Concede permissão para atualizar a configuração de versão de snapshot de perfil de segurança	Gravar	SecurityProfile*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pelo AWS Marketplace Vendor Insights

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Tipos de recursos	ARN	Chaves de condição
		aws:TagKeys

Chaves de condição do AWS Marketplace Vendor Insights

AWS Marketplace O Vendor Insights define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves de etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Mechanical Turk

O Amazon Mechanical Turk (prefixo do serviço: `mechanicalturk`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.

- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Mechanical Turk
- Tipos de recursos definidos pelo Amazon Mechanical Turk
- Chaves de condição do Amazon Mechanical Turk

Ações definidas pelo Amazon Mechanical Turk

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptQualificationRequest	A AcceptQualificationRequest operação concede a solicitação de qualificação de um trabalhador	Gravar			
ApproveAssignment	A ApproveAssignment operação aprova os resultados de uma tarefa concluída	Gravar			
AssociateQualificationWithWorker	A AssociateQualificationWithWorker operação confere ao trabalhador uma qualificação	Gravar			
CreateAdditionalAssignmentsForHIT	A operação CreateAdditionalAssignmentsFor HIT aumenta o número máximo de atribuições de um HIT existente	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateHIT	A operação CreateHIT cria uma nova HIT (Tarefa de inteligência humana)	Gravar			
CreateHITType	A HITType operação Create cria um novo tipo de HIT	Gravar			
CreateHITWithHITType	A HITWith HITType operação Create cria uma nova Human Intelligence Task (HIT) usando uma ID HITType existente gerada pela HITType operação Create	Gravar			
CreateQualificationType	A CreateQualificationType operação cria um novo tipo de qualificação, que é representado por uma estrutura QualificationType de dados	Gravar			
CreateWorkerBlock	A CreateWorkerBlock operação permite que você impeça que um trabalhador trabalhe em seu HITs	Gravar			
DeleteHIT	A operação DeleteHIT descarta uma HIT que não é mais necessária	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteQualificationType	O DeleteQualificationType dispõe de um tipo de qualificação e descarta todos os tipos de HIT associados ao tipo de qualificação	Gravar			
DeleteWorkerBlock	A DeleteWorkerBlock operação permite que você restabeleça um trabalhador bloqueado para trabalhar em seu HITs	Gravar			
DisassociateQualificationFromWorker	O DisassociateQualificationFromWorker revoga uma qualificação concedida anteriormente por um usuário	Gravar			
GetAccountBalance	A GetAccountBalance operação recupera a quantia em dinheiro em sua conta Amazon Mechanical Turk	Leitura			
GetAssignment	O GetAssignment recupera uma tarefa com um AssignmentStatus valor de Enviado, Aprovado ou Rejeitado, usando a ID da tarefa	Leitura			
GetFileUploadURL	A operação de GetFileUpload URL gera e retorna uma URL temporária	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetHIT	A operação GetHIT recupera os detalhes da HIT especificada	Leitura			
GetQualificationScore	A GetQualificationScore operação retorna o valor da Qualificação de um Trabalhador para um determinado tipo de Qualificação	Leitura			
GetQualificationType	A GetQualificationType operação recupera informações sobre um tipo de qualificação usando seu ID	Leitura			
ListAssignmentsForHIT	A operação ListAssignmentsFor HIT recupera atribuições concluídas para um HIT	Lista			
ListBonusPayments	A ListBonusPayments operação recupera os valores dos bônus que você pagou aos Trabalhadores por um determinado HIT ou tarefa	Lista			
ListHITs	A HITs operação List retorna todas as informações de um solicitante HITs	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListHITsForQualificationType	A HITs ForQualificationType operação List retorna o HITs que usa o fornecido QualififcationType para um QualificationRequirement	Lista			
ListQualificationRequests	A ListQualificationRequests operação recupera solicitações de qualificações de um determinado tipo de qualificação	Lista			
ListQualificationTypes	A ListQualificationTypes operação pesquisa os tipos de qualificação usando a consulta de pesquisa especificada e retorna uma lista dos tipos de qualificação	Lista			
ListReviewPolicyResultsForHIT	A operação ListReviewPolicyResultsFor HIT recupera os resultados computados e as ações tomadas durante a execução de suas políticas de revisão durante uma operação CreateHit.	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListReviewableHITs	A ListReviewable HITs operação retorna todas as informações de um solicitante HITs que não foram aprovadas ou rejeitadas	Lista			
ListWorkerBlocks	A ListWorkersBlocks operação recupera uma lista de trabalhadores que estão impedidos de trabalhar em seu HITs	Lista			
ListWorkersWithQualificationType	A ListWorkersWithQualificationType operação retorna todos os trabalhadores com um determinado tipo de qualificação	Lista			
NotifyWorkers	A NotifyWorkers operação envia um e-mail para um ou mais trabalhadores que você especifica com a ID do trabalhador	Gravar			
RejectAssignment	A RejectAssignment operação rejeita os resultados de uma tarefa concluída	Gravar			
RejectQualificationRequest	A RejectQualificationRequest operação rejeita a solicitação de qualificação de um usuário	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SendBonus	A SendBonus operação emite um pagamento em dinheiro da sua conta para um trabalhador	Gravar			
SendTestEventNotification	A SendTestEventNotification operação faz com que o Amazon Mechanical Turk envie uma mensagem de notificação como se um evento HIT tivesse ocorrido, de acordo com a especificação de notificação fornecida.	Gravar			
UpdateExpirationForHIT	A operação UpdateExpirationFor HIT permite estender o tempo de expiração de um HIT além da expiração atual ou expirar um HIT imediatamente.	Gravar			
UpdateHITReviewStatus	A operação Atualizar HITReview status alterna o status de um HIT	Gravar			
UpdateHITTypeOfHIT	A operação Update HITTypeofHit permite que você altere as HITType propriedades de um HIT	Gravar			
UpdateNotificationSettings	A UpdateNotificationSettings operação cria, atualiza, desativa ou reativa notificações para um tipo de HIT	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateQualificationType	A UpdateQualificationType operação modifica os atributos de um tipo de qualificação existente, que é representado por uma estrutura de QualificationType dados	Gravar			

Tipos de recursos definidos pelo Amazon Mechanical Turk

O Amazon Mechanical Turk não oferece suporte à especificação de um ARN de recurso no elemento `Resource` de uma declaração de política do IAM. Para permitir o acesso ao Amazon Mechanical Turk, especifique `"Resource": "*"` em sua política.

Chaves de condição do Amazon Mechanical Turk

MechanicalTurk não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o Amazon MemoryDB

O Amazon MemoryDB (prefixo do serviço: `memorydb`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon MemoryDB

- Tipos de recursos definidos pelo Amazon MemoryDB
- Chaves de condição para o Amazon MemoryDB

Ações definidas pelo Amazon MemoryDB

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

> **Note**
>
> Ao criar uma política do Amazon MemoryDB for Redis no IAM, é necessário usar o caractere curinga "*" para o bloco de recursos. Para obter informações sobre como usar as seguintes ações de API do MemoryDB for Redis em uma política do IAM, consulte Ações do MemoryDB e IAM.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchUpdateCluster	Concede permissões para aplicar atualizações de serviço	Gravar	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					s3:GetObject
				aws:ResourceTag/${TagKey}	
Connect	Permite que um perfil ou usuário do IAM se conecte como um usuário especificado do MemoryDB a um nó em um cluster	Gravar	cluster*		
			user*		
				aws:ResourceTag/${TagKey}	
CopySnapshot	Concede permissões para fazer uma cópia de um snapshot existente	Gravar	snapshot*		memorydb:TagResource s3:DeleteObject s3:GetBucketAcl s3:PutObject

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateAcl	Concede permissões para criar uma nova lista de controle de acesso	Gravar	user*		memorydb:TagResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateCluster	Concede permissões para criar um cluster	Gravar	acl*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs memorydb:TagResource s3:GetObject
			parametergroup*		
			subnetgroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			multiregioncluster		
			snapshot		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys memorydb:TLSEnabled	
CreateMultiRegionCluster	Concede permissões para criar um cluster multirregional	Gravar	multiregionparametergroup*		memorydb:TagResource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys memorydb:TLSEnabled	
CreateParameterGroup	Concede permissões para criar um novo grupo de parâmetros	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	memorydb:TagResource
CreateSnapshot	Concede permissões para criar um backup de um cluster no momento atual	Gravar	cluster*		memorydb:TagResource s3:DeleteObject s3:GetBucketAcl s3:PutObject

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubnetGroup	Concede permissões para criar um novo grupo de sub-redes	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	memorydb:TagResource
CreateUser	Concede permissões para criar um novo usuário	Gravar		aws:RequestTag/${TagKey} aws:TagKeys memorydb:UserAuthenticationMode	memorydb:TagResource
DeleteAcl	Concede permissões para excluir uma lista de controle de acesso	Gravar	acl*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
DeleteCluster	Concede permissões para excluir um cluster provisionado anteriormente	Gravar	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			multiregioncluster		
			snapshot		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteMultiRegionCluster	Concede permissões para excluir um cluster multirregional	Gravar	multiregioncluster*		
				aws:ResourceTag/${TagKey}	
DeleteParameterGroup	Concede permissões para criar um grupo de parâmetros	Gravar	parametergroup*		
				aws:ResourceTag/${TagKey}	
DeleteSnapshot	Concede permissões para excluir um snapshot	Gravar	snapshot*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteSubnetGroup	Concede permissões para excluir um grupo de sub-redes	Gravar	subnetgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	
DeleteUser	Concede permissões para excluir um usuário	Gravar	user*		
				aws:ResourceTag/${TagKey}	
DescribeAcls	Concede permissões para recuperar informações sobre listas de controle de acesso	Leitura	acl*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
DescribeClusters	Concede permissões para recuperar informações sobre todos os clusters provisionados se nenhum identificador de cluster for especificado, ou sobre um cluster específico, se um identificador de cluster for fornecido	Leitura	cluster*		
				aws:ResourceTag/${TagKey}	
DescribeEngineVersions	Concede permissões para listar os mecanismos disponíveis e suas versões	Leitura			
DescribeEvents	Concede permissões para recuperar eventos relacionados a clusters, grupos de sub-redes e grupos de parâmetros	Leitura			
DescribeMultiRegionClusters	Concede permissões para recuperar informações sobre todos os clusters multirregionais se nenhum identificador de cluster for especificado ou sobre um cluster multirregional específico se um identificador de cluster for fornecido	Leitura	multiregioncluster*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeMultiRegionParameterGroups	Concede permissões para recuperar informações sobre grupos de parâmetros multirregionais	Leitura	multiregionparametergroup*		
DescribeMultiRegionParameters	Concede permissões para recuperar uma lista de parâmetros detalhada para um determinado grupo de parâmetros multirregionais	Leitura	multiregionparametergroup*		
DescribeParameterGroups	Concede permissões para recuperar informações sobre grupos de parâmetros	Leitura	parametergroup*		
				aws:ResourceTag/${TagKey}	
DescribeParameters	Concede permissões para recuperar uma lista de parâmetros detalhada para um determinado grupo de parâmetros	Leitura	parametergroup*		
				aws:ResourceTag/${TagKey}	
DescribeReservedNodes	Concede permissões para recuperar os nós reservados	Leitura	reservednode*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeReservedNodesOfferings	Concede permissões para recuperar as ofertas de nós reservados	Leitura			
DescribeServiceUpdates	Concede permissões para recuperar os detalhes de atualizações do serviço	Leitura			
DescribeSnapshots	Concede permissões para recuperar informações sobre snapshots de cluster	Leitura	snapshot*		
				aws:ResourceTag/${TagKey}	
DescribeSubnetGroups	Concede permissões para recuperar um grupo de sub-redes	Leitura	subnetgroup*		
				aws:ResourceTag/${TagKey}	
DescribeUsers	Concede permissões para recuperar informações sobre usuários	Leitura	user*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
FailoverShard	Concede permissões para testar failover automático em um fragmento especificado em um cluster	Gravar	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	
ListAllowedMultiRegionClusterUpdates	Concede permissões para listar as atualizações de clusters multirregionais disponíveis	Leitura	multiregioncluster*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAllowedNodeTypeUpdates	Concede permissões para listar atualizações de tipo de nó disponíveis	Leitura	cluster*		
				aws:ResourceTag/${TagKey}	
ListTags	Concede permissões para listar todas as etiquetas de alocação de custo	Leitura	acl		
			cluster		
			multiregioncluster		
			parametergroup		
			snapshot		
			subnetgroup		
			user		
				aws:ResourceTag/${TagKey}	
PauseMultiRegionClusterReplication [somente permissão]	Concede permissão para pausar a replicação para um cluster multirregional	Gravar	multiregioncluster*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PurchaseReservedNodesOffering	Concede permissões para adquirir um novo nó reservado	Gravar	reservednode*		memorydb:TagResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
ResetParameterGroup	Concede permissões para modificar os parâmetros de um grupo de parâmetros para o valor padrão do mecanismo ou do sistema	Gravar	parametergroup*		
				aws:ResourceTag/${TagKey}	
TagResource	Concede permissões para adicionar até 10 etiquetas de alocação de custo ao recurso nomeado	Tags	acl		
			cluster		
			multiregioncluster		
			parametergroup		
			reservednode		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			snapshot		
			subnetgroup		
			user		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permissões para remover as tags identificadas pela TagKeys lista de um recurso	Tags	acl		
			cluster		
			multiregioncluster		
			parametergroup		
			snapshot		
			subnetgroup		
			user		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateAcl	Concede permissões para atualizar uma lista de controle de acesso	Gravar	acl*		
			user*		
				aws:ResourceTag/${TagKey}	
UpdateCluster	Concede permissões para atualizar as configurações de um cluster	Gravar	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			acl		
			parameter group		
				aws:ResourceTag/${TagKey}	
UpdateMultiRegionCluster	Concede permissões para atualizar as configurações de um cluster multirregional	Gravar	multiregioncluster *		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			multiregionparametergroup		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
UpdateParameterGroup	Concede permissões para atualizar os parâmetros em um grupo de parâmetros	Gravar	parametergroup*		
				aws:ResourceTag/${TagKey}	
UpdateSubnetGroup	Concede permissões para atualizar um grupo de sub-redes	Gravar	subnetgroup*		
				aws:ResourceTag/${TagKey}	
UpdateUser	Concede permissões para atualizar um usuário	Gravar	user*		
				aws:ResourceTag/${TagKey} memorydb:UserAuthenticationMode	

Tipos de recursos definidos pelo Amazon MemoryDB

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações

identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
reservednode	`arn:${Partition}:memorydb:${Region}:${Account}:reservednode/${ReservationID}`	aws:ResourceTag/${TagKey}

Chaves de condição para o Amazon MemoryDB

O Amazon MemoryDB define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra ações com base nas etiquetas transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra as ações com base nas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra ações com base nas chaves da etiqueta transmitidas na solicitação	ArrayOfString
memorydb:TLSEnabled	Filtra o acesso pelo TLSEnabled parâmetro presente na solicitação ou assume como padrão o valor verdadeiro se o parâmetro não estiver presente	Bool
memorydb:UserAuthenticationMode	Filtra o acesso pelo parâmetro UserAuthentication Mode .Type na solicitação	String

Ações, recursos e chaves de condição do Serviço de entrega de mensagens da Amazon

O Serviço de entrega de mensagens da Amazon (prefixo do serviço: `ec2messages`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Serviço de entrega de mensagens da Amazon
- Tipos de recursos definidos pelo Serviço de entrega de mensagens da Amazon
- Chaves de condição do Serviço de entrega de mensagens da Amazon

Ações definidas pelo Serviço de entrega de mensagens da Amazon

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar

a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcknowledgeMessage	Concede permissão para confirmar uma mensagem, garantindo que ela não será entregue novamente	Write			
DeleteMessage	Concede permissão para excluir uma mensagem	Write			
FailMessage	Concede permissão para reprovar uma mensagem, o que significa que a mensagem	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	não pôde ser processada com sucesso, garantindo que ela não possa ser respondida ou entregue novamente				
GetEndpoint	Concede permissão para rotear o tráfego para o endpoint correto baseado no destino dado para as mensagens	Leitura			
GetMessages	Concede permissão para enviar mensagens clients/instances usando uma sondagem longa	Leitura		ssm:SourceInstanceARN ec2:SourceInstanceARN	
SendReply	Concede permissão para enviar respostas do serviço clients/instances upstream	Gravar		ssm:SourceInstanceARN ec2:SourceInstanceARN	

Tipos de recursos definidos pelo Serviço de entrega de mensagens da Amazon

O Serviço de entrega de mensagens da Amazon não oferece suporte à especificação do ARN de um recurso no elemento `Resource` de uma instrução de política do IAM. Para conceder acesso ao Serviço de entrega de mensagens da Amazon, especifique `"Resource": "*"` na política.

Chaves de condição do Serviço de entrega de mensagens da Amazon

O Amazon Message Delivery Service define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
ec2:SourceInstanceARN	Filtra o acesso pelo ARN da instância da qual a solicitação se originou.	ARN
ssm:SourceInstanceARN	Filtra o acesso verificando o Amazon Resource Name (ARN) da instância gerenciada AWS do Systems Manager a partir da qual a solicitação é feita. Essa chave não está presente quando a solicitação vem da instância gerenciada autenticada com uma função do IAM associada ao perfil da EC2 instância.	ARN

Ações, recursos e chaves de condição do Amazon Message Gateway Service

O Amazon Message Gateway Service (prefixo do serviço: `ssmmessages`) fornece os recursos, ações e chaves de contexto de condição a seguir específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Message Gateway Service
- Tipos de recursos definidos pelo Amazon Message Gateway Service
- Chaves de condição do Amazon Message Gateway Service

Ações definidas pelo Amazon Message Gateway Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de

recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateControlChannel	Concede permissão para registrar um canal de controle para uma instância para enviar mensagens de controle para o serviço Systems Manager	Write		ssm:SourceInstanceARN ec2:SourceInstanceARN	
CreateDataChannel	Concede permissão para registrar um canal de dados para uma instância para enviar mensagens de dados para o serviço Systems Manager	Write			
OpenControlChannel	Concede permissão para abrir uma conexão websocket para um fluxo de canal de controle registrado de uma instância para o serviço Systems Manager	Write			
OpenDataChannel	Concede permissão para abrir uma conexão websocket para um fluxo de canal de dados registrado de uma instância	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	para o serviço Systems Manager				

Tipos de recursos definidos pelo Amazon Message Gateway Service

O Amazon Message Gateway Service não oferece suporte à especificação do ARN de um recurso no elemento `Resource` de uma instrução de política do IAM. Para conceder acesso ao Amazon Message Gateway Service, especifique `"Resource": "*"` na política.

Chaves de condição do Amazon Message Gateway Service

O Amazon Message Gateway Service define as chaves de condição a seguir que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
ec2:SourceInstanceARN	Filtra o acesso pelo ARN da instância da qual a solicitação se originou.	ARN
ssm:SourceInstanceARN	Filtra o acesso verificando o Amazon Resource Name (ARN) da instância gerenciada AWS do Systems Manager a partir da qual a solicitação é feita. Essa chave não está presente quando a solicitação vem da instância gerenciada autenticada com uma função do IAM associada ao perfil da EC2 instância.	ARN

Ações, recursos e chaves de condição para o AWS Microservice Extractor for .NET

AWS O Microservice Extractor for .NET (prefixo do serviço:`serviceextract`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Microservice Extractor for .NET
- Tipos de recursos definidos por AWS Microservice Extractor for .NET
- Chaves de condição para o AWS Microservice Extractor for .NET

Ações definidas pelo AWS Microservice Extractor for .NET

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa

ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetConfig [somente permissão]	Concede permissão para obter a configuração necessária para o cliente de AWS desktop Microservice Extractor for .NET	Leitura			

Tipos de recursos definidos por AWS Microservice Extractor for .NET

AWS O Microservice Extractor para.NET não oferece suporte à especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para permitir ao acesso ao AWS Microservice Extractor for .NET, especifique `"Resource": "*"` em sua política.

Chaves de condição para o AWS Microservice Extractor for .NET

O Microservice Extractor for .NET não tem chaves de contexto específicas ao serviço que possam ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para créditos do Programa de Aceleração da Migração da AWS

AWS Os créditos do Migration Acceleration Program (prefixo do serviço:`mapcredits`) fornecem os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas por créditos do Programa de Aceleração da Migração da AWS
- Tipos de recursos definidos por créditos do Programa de Aceleração da Migração da AWS
- Chaves de condição para créditos do Programa de Aceleração da Migração da AWS

Ações definidas por créditos do Programa de Aceleração da Migração da AWS

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou

ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAssociatedPrograms [somente permissão]	Concede permissão para visualizar os contratos do Programa de Aceleração de Migração associados do usuário	Lista	agreement*		
ListQuarterCredits [somente permissão]	Concede permissão para visualizar créditos de contratos do Programa de Aceleração da Migração associados à conta pagante do usuário	Lista	agreement*		
ListQuarterSpend [somente permissão]	Concede permissão para visualizar gastos elegíveis de contratos do Programa de Aceleração da Migração associados à conta pagante do usuário	Lista	agreement*		

Tipos de recursos definidos por créditos do Programa de Aceleração da Migração da AWS

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
agreement	`arn:${Partition}:mapcredits:::${Agreement}/${AgreementId}`	

Chaves de condição para créditos do Programa de Aceleração da Migração da AWS

MapCredits não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Migration Hub

AWS O Migration Hub (prefixo do serviço:`mgh`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Migration Hub
- Tipos de recursos definidos pelo AWS Migration Hub
- Chaves de condição do AWS Migration Hub

Ações definidas pelo AWS Migration Hub

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptConnection	Concede permissão para aceitar uma conexão	Gravar	ConnectionResource*		
				aws:TagKeys aws:RequestTag/${TagKey}	
AssociateAutomationUnitRole	Concede permissão para associar uma função do IAM a uma unidade de automação	Gravar	AutomationUnitResource*		
AssociateCreatedArtifact	Concede permissão para associar um determinado AWS artefato a um Migration Task	Gravar	migrationTask*		
AssociateDiscoveredResource	Concede permissão para associar um determinado recurso do ADS a um MigrationTask	Gravar	migrationTask*		
AssociateSourceResource	Concede permissão para associar o recurso de origem	Gravar	migrationTask*		
BatchAssociateIamRoleWithConnection	Concede permissão para associar em lote funções do IAM a uma conexão	Gravar	ConnectionResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchDisassociateIamRoleFromConnection	Concede permissão para desassociar em lote as funções do IAM de uma conexão	Gravar	ConnectionResource*		
CreateAutomationRun	Concede permissão para criar uma execução de unidade de automação	Gravar			
CreateAutomationUnit	Concede permissão para criar uma unidade de automação	Gravar			
CreateHomeRegionControl	Concede permissão para criar um controle de região de origem do Migration Hub	Gravar			
CreateProgressUpdateStream	Concede permissão para criar um ProgressUpdateStream	Gravar	progressUpdateStream*		
DeleteAutomationRun	Concede permissão para excluir uma execução de unidade de automação	Gravar	AutomationRunResource*		
DeleteAutomationUnit	Concede permissão para excluir uma unidade de automação	Gravar	AutomationUnitResource*		
DeleteConnection	Concede permissão para excluir uma conexão	Gravar	ConnectionResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteHomeRegionControl	Concede permissão para excluir um controle de região de origem do Migration Hub	Gravar			
DeleteProgressUpdateStream	Concede permissão para excluir um ProgressUpdateStream	Gravar	progressUpdateStream*		
DescribeApplicationState	Concede permissão para obter o estado de uma aplicação do Application Discovery Service	Leitura			
DescribeAutomationRun	Concede permissão para descrever a execução de uma unidade de automação	Leitura	AutomationRunResource*		
DescribeAutomationUnit	Concede permissão para descrever uma unidade de automação	Leitura	AutomationUnitResource*		
DescribeHomeRegionControls	Concede permissão para listar controles de região de origem	Lista			
DescribeMigrationTask	Concede permissão para descrever um MigrationTask	Leitura	migrationTask*		
DisassociateAutomationUnitRole	Concede permissão para desassociar uma função do IAM de uma unidade de automação	Gravar	AutomationUnitResource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateCreatedArtifact	Concede permissão para desassociar um determinado AWS artefato de um Migration Task	Gravar	migrationTask*		
DisassociateDiscoveredResource	Concede permissão para desassociar um determinado recurso do ADS de um MigrationTask	Gravar	migrationTask*		
DisassociateSourceResource	Concede permissão para desassociar o recurso de origem	Gravar	migrationTask*		
GetConnection	Concede permissão para obter uma conexão	Leitura	ConnectionResource*		
GetHomeRegion	Concede permissão para obter a região de origem do Migration Hub	Leitura			
ImportMigrationTask	Concede permissão para importar um MigrationTask	Gravar	migrationTask*		
ListApplicationStates	Concede permissão para listar status de aplicações	Lista			
ListAutomationRuns	Concede permissão para listar execuções de unidades de automação	Lista			
ListAutomationUnits	Concede permissão para listar unidades de automação	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListConnectionRoles	Concede permissão para listar funções de conexão	Lista	ConnectionResource*		
ListConnections	Concede permissão para listar conexões	Lista			
ListCreatedArtifacts	Concede permissão para listar artefatos criados associados para um MigrationTask	Lista	migrationTask*		
ListDiscoveredResources	Concede permissão para listar recursos ADS associados de MigrationTask	Lista	migrationTask*		
ListMigrationTaskUpdates	Concede permissão para listar atualizações de tarefas de migração	Lista	migrationTask*		
ListMigrationTasks	Concede permissão para listar MigrationTasks	Lista			
ListProgressUpdateStreams	Concede permissão para listar ProgressUpdateStreams	Lista			
ListSourceResources	Concede permissão para listar recursos de origem	Lista	migrationTask*		
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
NotifyApplicationState	Concede permissão para atualizar o estado de uma aplicação do Application Discovery Service	Gravar			
NotifyMigrationTaskState	Concede permissão para notificar o MigrationTask estado mais recente	Gravar	migrationTask*		
PutResourceAttributes	Concede permissão para colocar ResourceAttributes	Gravar	migrationTask*		
RejectConnection	Concede permissão para rejeitar uma conexão	Gravar	ConnectionResource*		
TagResource	Concede permissão para marcar um recurso	Marcação		aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para desmarcar um recurso	Tags		aws:TagKeys	

Tipos de recursos definidos pelo AWS Migration Hub

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves

são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
progressUpdateStream	`arn:${Partition}:mgh:${Region}:${Account}:progressUpdateStream/${Stream}`	
migrationTask	`arn:${Partition}:mgh:${Region}:${Account}:progressUpdateStream/${Stream}/migrationTask/${Task}`	
AutomationRunResource	`arn:${Partition}:mgh:${Region}:${Account}:automation-run/${RunID}`	mgh:AutomationRunResourceRunID
AutomationUnitResource	`arn:${Partition}:mgh:${Region}:${Account}:automation-unit/${AutomationUnitId}`	mgh:AutomationUnitResourceAutomationUnitArn
ConnectionResource	`arn:${Partition}:mgh:${Region}:${Account}:${ConnectionArn}`	aws:ResourceTag/${TagKey} mgh:ConnectionResourceConnectionArn

Chaves de condição do AWS Migration Hub

AWS O Migration Hub define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base nas etiquetas transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra as ações com base nas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra ações com base nas chaves da etiqueta transmitidas na solicitação	ArrayOfString
mgh:AutomationRunResourceRunID	AutomationRunResource identificador RunID do recurso	String
mgh:AutomationUnitResourceAutomationUnitArn	AutomationUnitResource automationUnitArn identificador de recurso	ARN
mgh:ConnectionResourceConnectionArn	ConnectionResource identificador de conexão de recursos/ARN	String

Ações, recursos e chaves de condição do AWS Migration Hub Orchestrator

AWS O Migration Hub Orchestrator (prefixo do serviço:`migrationhub-orchestrator`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.

- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Migration Hub Orchestrator
- Tipos de recursos definidos pelo AWS Migration Hub Orchestrator
- Chaves de condição para o AWS Migration Hub Orchestrator

Ações definidas pelo AWS Migration Hub Orchestrator

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateTemplate	Concede permissão para criar um modelo personalizado	Gravar			
CreateWorkflow	Concede permissão para criar um fluxo de trabalho com base no modelo selecionado	Gravar	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkflowStep	Concede permissão para criar uma etapa em um fluxo de trabalho e em um grupo de etapas específico	Gravar	workflow*		
CreateWorkflowStepGroup	Concede permissão para criar um grupo de etapas personalizado para determinado fluxo de trabalho	Gravar	workflow*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteTemplate	Concede permissão para excluir um modelo personalizado	Gravar	template*		
DeleteWorkflow	Concede permissão para um fluxo de trabalho	Gravar	workflow*		
DeleteWorkflowStep	Concede permissão para excluir uma etapa de um grupo de etapas específico de um fluxo de trabalho	Gravar	workflow*		
DeleteWorkflowStepGroup	Concede permissão para excluir um grupo de etapas associado a um fluxo de trabalho	Gravar	workflow*		
GetMessage	Concede permissão ao plugin para receber informações do serviço	Leitura			
GetTemplate	Concede permissão para obter metadados recuperados de um modelo	Leitura	template*		
GetTemplateStep	Concede permissão para recuperar detalhes de uma etapa associada a um modelo e um grupo de etapas	Leitura	template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetTemplateStepGroup	Concede permissão para recuperar metadados de um grupo de etapas de um modelo	Leitura	template*		
GetWorkflow	Concede permissão para recuperar metadados associados a um fluxo de trabalho	Leitura	workflow*		
GetWorkflowStep	Concede permissão para obter detalhes de uma etapa associada a um fluxo de trabalho e a um grupo de etapas	Leitura	workflow*		
GetWorkflowStepGroup	Concede permissão para obter detalhes de um grupo de etapas associado a um fluxo de trabalho	Leitura	workflow*		
ListPlugins	Concede permissão para obter uma lista de todos os plugins registrados	Lista			
ListTagsForResource	Concede permissão para obter uma lista de todas as etiquetas vinculadas a um recurso	Leitura	template* workflow*		
ListTemplateStepGroups	Concede permissão para listar grupos de etapas de um modelo	Lista	template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTemplateSteps	Concede permissão para obter uma lista de etapas de um grupo	Lista	template*		
ListTemplates	Concede permissão para obter uma lista de todos os modelos disponíveis para o cliente	Lista			
ListWorkflowStepGroups	Concede permissão para obter uma lista de grupos de etapas associados a um fluxo de trabalho	Lista	workflow*		
ListWorkflowSteps	Concede permissão para obter uma lista de etapas em um grupo de etapas associado a um fluxo de trabalho	Lista	workflow*		
ListWorkflows	Concede permissão para listar todos os fluxos de trabalho	Lista			
RegisterPlugin	Concede permissão para registrar o plugin para receber um ID e iniciar o recebimento de mensagens do serviço	Gravar			
RetryWorkflowStep	Concede permissão para repetir uma etapa com falha em um fluxo de trabalho	Gravar	workflow*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SendMessage	Concede permissão ao plugin para enviar informações ao serviço	Gravar			
StartWorkflow	Concede permissão para iniciar um fluxo de trabalho ou retomar um fluxo de trabalho interrompido	Gravar	workflow*		
StopWorkflow	Concede permissão para interromper um fluxo de trabalho	Gravar	workflow*		
TagResource	Concede permissão para adicionar tags a um recurso	Marcação	template		
			workflow		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover etiquetas de um recurso	Tags	template		
			workflow		
				aws:TagKeys	
UpdateTemplate	Concede permissão para atualizar um modelo personalizado	Gravar	template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateWorkflow	Concede permissão para atualizar os metadados associados ao fluxo de trabalho	Gravar	workflow*		
UpdateWorkflowStep	Concede permissão para atualizar metadados e status de uma etapa personalizada em um fluxo de trabalho	Gravar	workflow*		
UpdateWorkflowStepGroup	Concede permissão para atualizar metadados associados a um grupo de etapas em determinado fluxo de trabalho	Gravar	workflow*		

Tipos de recursos definidos pelo AWS Migration Hub Orchestrator

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
workflow	`arn:${Partition}:migrationhub-orchestrator:${Region}:${Account}:workflow/${ResourceId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
template	`arn:${Partition}:migrationhub-orchestrator:${Region}:${Account}:template/${ResourceId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o AWS Migration Hub Orchestrator

AWS O Migration Hub Orchestrator define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Migration Hub Refactor Spaces

AWS O Migration Hub Refactor Spaces (prefixo do serviço:`refactor-spaces`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Migration Hub Refactor Spaces
- Tipos de recursos definidos pelo AWS Migration Hub Refactor Spaces
- Chaves de condição do AWS Migration Hub Refactor Spaces

Ações definidas pelo AWS Migration Hub Refactor Spaces

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateApplication	Concede permissão para criar uma aplicação dentro de um ambiente	Gravar		refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateEnvironment	Concede permissão para criar um ambiente	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateRoute	Concede permissão para criar uma rota dentro de uma aplicação	Gravar		refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateService	Concede permissão para criar um serviço dentro de uma aplicação	Gravar		refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:CreatedByAccountIds aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Concede permissão para excluir uma aplicação de um ambiente	Gravar	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds aws:ResourceTag/${TagKey}	
DeleteEnvironment	Concede permissão para excluir um ambiente	Gravar	environment*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	Concede permissão para excluir uma política de recurso	Gravar			
DeleteRoute	Concede permissão para excluir uma rota de uma aplicação	Gravar	route*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:ResourceTag/${TagKey}	
DeleteService		Gravar	service*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	Concede permissão para excluir um serviço de uma aplicação			refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:CreatedByAccountIds aws:ResourceTag/${TagKey}	
GetApplication	Concede permissão para obter mais informações sobre uma aplicação	Leitura	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds aws:ResourceTag/${TagKey}	
GetEnvironment	Concede permissão para obter informações para um ambiente	Leitura	environment*		
				aws:ResourceTag/${TagKey}	
GetResourcePolicy	Concede permissão para obter detalhes sobre uma política de recurso	Leitura			
GetRoute	Concede permissão para obter mais informações sobre uma rota	Leitura	route*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetService	Concede permissão para obter mais informações sobre um serviço	Leitura	service*		
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:CreatedByAccountIds aws:ResourceTag/${TagKey}	
ListApplications	Concede permissão para listar as aplicações em um ambiente	Leitura	application*		
ListEnvironmentVpcs	Concede permissão para listar todos VPCs os do ambiente	Leitura	environment*		
ListEnvironments	Concede permissão para listar todos os ambientes	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListRoutes	Concede permissão para listar todas as rotas em uma aplicação	Leitura	route*		
ListServices	Concede permissão para listar todos os serviços em um ambiente	Leitura	environment*		
ListTagsForResource	Concede permissão para listar todas as etiquetas para determinado recurso	Leitura			
PutResourcePolicy	Concede permissão para adicionar uma política de recurso	Gravar			
TagResource	Concede permissão para marcar um recurso	Tags	application		
			environment		
			route		
			service		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
UntagResource	Concede permissão para remover uma etiqueta de um recurso	Tags	application		
			environment		
			route		
			service		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
UpdateRoute	Concede permissão para atualizar uma rota de uma aplicação	Gravar	route*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pelo AWS Migration Hub Refactor Spaces

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
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

Chaves de condição do AWS Migration Hub Refactor Spaces

AWS O Migration Hub Refactor Spaces define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString
refactor-spaces:ApplicationCreatedByAccount	Filtra o acesso restringindo a ação somente àquelas contas que criaram a aplicação em um ambiente	String
refactor-spaces:CreatedByAccountIds	Filtra o acesso pelas contas que criaram o recurso	ArrayOfString
refactor-spaces:RouteCreatedByAccount	Filtra o acesso restringindo a ação somente àquelas contas que criaram a rota dentro de uma aplicação	String
refactor-spaces:ServiceCreatedByAccount	Filtra o acesso restringindo a ação somente àquelas contas que criaram o serviço dentro de uma aplicação	String
refactor-spaces:SourcePath	Filtra o acesso pelo caminho da rota	String

Ações, recursos e chaves de condição para o AWS Migration Hub Strategy Recommendations

AWS As recomendações de estratégia do Migration Hub (prefixo do serviço:`migrationhub-strategy`) fornecem os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Migration Hub Strategy Recommendations
- Tipos de recursos definidos pelo AWS Migration Hub Strategy Recommendations
- Chaves de condição para o AWS Migration Hub Strategy Recommendations

Ações definidas pelo AWS Migration Hub Strategy Recommendations

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa

ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAntiPattern	Concede permissão para obter detalhes de cada antipadrão que o coletor deve examinar no ambiente de um cliente	Leitura			
GetApplicationComponentDetails	Concede permissão para obter os detalhes de uma aplicação	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetApplicationComponentStrategies	Concede permissão para obter uma lista de todas as estratégias e ferramentas recomendadas para uma aplicação em execução em um servidor	Leitura			
GetAssessment	Concede permissão para recuperar o status de uma avaliação em andamento	Leitura			
GetImportFileTask	Concede permissão para obter detalhes de uma tarefa de importação específica	Leitura			
GetLatestAssessmentId	Concede permissão para recuperar o ID de avaliação mais recente	Leitura			
GetMessage	Concede permissão ao coletor para receber informações do serviço	Leitura			
GetPortfolioPreferences	Concede permissão para recuperar as preferências do cliente migration/Modernization	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetPortfolioSummary	Concede permissão para recuperar o resumo geral (número de servidores para redefinir a hospedagem, etc, bem como o número geral de antipadrões)	Leitura			
GetRecommendationReportDetails	Concede permissão para recuperar informações detalhadas sobre um relatório de recomendações	Leitura			
GetServerDetails	Concede permissão para obter informações sobre um servidor específico	Leitura			
GetServerStrategies	Concede permissão para obter estratégias e ferramentas recomendadas para um servidor específico	Leitura			
ListAnalyzableServers	Concede permissão para obter uma lista de todos os servidores analisáveis no ambiente vcenter de um cliente	Lista			
ListAntiPatterns	Concede permissão para obter uma lista de todos os antipadrões que o coletor deve procurar no ambiente de um cliente	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListApplicationComponents	Concede permissão para obter uma lista de todas as aplicações em execução em servidores do cliente	Lista			
ListCollectors	Concede permissão para obter uma lista de todos os coletores instalados pelo cliente	Lista			
ListImportFileTask	Concede permissão para obter uma lista de todas as importações realizadas pelo cliente	Lista			
ListJarArtifacts	Concede permissão para obter uma lista de binários que o coletor deve avaliar	Lista			
ListServers	Concede permissão para obter uma lista de todos os servidores no ambiente de um cliente	Lista			
PutLogData	Concede permissão ao coletor para enviar logs ao serviço	Gravar			
PutMetricData	Concede permissão ao coletor para enviar métricas ao serviço	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutPortfolioPreferences	Concede permissão para salvar Migration/Modernization as preferências do cliente	Gravar			
RegisterCollector	Concede permissão para registrar o coletor para receber uma ID e iniciar o recebimento de mensagens do serviço	Gravar			
SendMessage	Concede permissão ao coletor para enviar informações ao serviço	Gravar			
StartAssessment	Concede permissão para iniciar a avaliação no ambiente de um cliente (coletar dados de todos os servidores e fornecer recomendações)	Gravar			
StartImportFileTask	Concede permissão para começar a importar dados de um arquivo fornecido pelo cliente	Gravar			
StartRecommendationReportGeneration	Concede permissão para começar a gerar um relatório de recomendações	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopAssessment	Concede permissão para interromper uma avaliação em andamento	Gravar			
UpdateApplicationComponentConfig	Concede permissão para atualizar os detalhes de uma aplicação	Gravar			
UpdateCollectorConfiguration	Concede permissão ao coletor para enviar informações de configuração ao serviço	Gravar			
UpdateServerConfig	Concede permissão para atualizar informações em um servidor junto com a estratégia recomendada	Gravar			

Tipos de recursos definidos pelo AWS Migration Hub Strategy Recommendations

AWS O Migration Hub Strategy Recommendations não suporta a especificação de um ARN de recurso `Resource` no elemento de uma declaração de política do IAM. Para permitir ao acesso ao AWS Migration Hub Strategy Recommendations, especifique `"Resource": "*"` na política.

Chaves de condição para o AWS Migration Hub Strategy Recommendations

O Migration Hub Strategy Recommendations não tem chaves de contexto específicas de serviço que podem ser usadas no elemento `Condition` das instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do Amazon Mobile Analytics

O Amazon Mobile Analytics (prefixo do serviço: `mobileanalytics`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Mobile Analytics
- Tipos de recursos definidos pelo Amazon Mobile Analytics
- Chaves de condição do Amazon Mobile Analytics

Ações definidas pelo Amazon Mobile Analytics

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar

a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetFinancialReports	Conceder acesso às métricas financeiras para um aplicativo	Read			
GetReports	Conceder acesso às métricas padrão para um aplicativo	Leitura			
PutEvents	A PutEvents operação registra um ou mais eventos	Gravar			

Tipos de recursos definidos pelo Amazon Mobile Analytics

O Amazon Mobile Analytics não oferece suporte à especificação do ARN de um recurso no elemento `Resource` de uma instrução de política do IAM. Para conceder acesso ao Amazon Mobile Analytics, especifique `"Resource": "*"` na política.

Chaves de condição do Amazon Mobile Analytics

O Mobile Analytics não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o Amazon Monitron

O Amazon Monitron (prefixo de serviço: `monitron`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de IAM permissão.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Monitron
- Tipos de recursos definidos pelo Amazon Monitron
- Chaves de condição para o Amazon Monitron

Ações definidas pelo Amazon Monitron

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateProjectAdminUser [somente permissão]	Concede permissão para associar um usuário ao projeto como administrador	Permissions management	project*		sso-directory:DescribeUsers sso:AssociateProfile sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfileAssociations sso:ListProfiles
CreateProject [somente permissão]	Concede permissão para criar um projeto	Gravação		aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole kms:CreateGrant

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					sso:CreateManagedApplicationInstance sso:DeleteManagedApplicationInstance sso:DescribeRegisteredRegions

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateProjectUserAssociation [somente permissão]	Concede permissão para associar um usuário ao projeto	Gerenciamento de permissões	project*		sso-directory:DescribeUsers sso:AssociateProfile sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfileAssociations sso:ListProfiles

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateUserAccessRoleAssociation [somente permissão]	Concede permissão para associar um perfil de acesso ao usuário	Gerenciamento de permissões	project*		sso-directory:DescribeUsers sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfileAssociations sso:ListProfiles
DeleteProject [somente permissão]	Concede permissão para excluir um projeto	Write	project*		sso:DeleteManagedApplicationInstance

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteProjectUserAssociation [somente permissão]	Concede permissão para desassociar um usuário do projeto	Gerenciamento de permissões	project*		sso-directory:DescribeUsers sso:DisassociateProfile sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfiles
DeleteUserAccessRoleAssociation [somente permissão]	Concede permissão para desassociar um perfil de acesso do usuário	Gerenciamento de permissões	project*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateProjectAdminUser [somente permissão]	Concede permissão para desassociar um administrador do projeto	Permissions management	project*		sso-directory:DescribeUsers sso:DisassociateProfile sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfiles
GetProject [somente permissão]	Concede permissão para obter informações sobre um projeto	Read	project*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetProjectAdminUser [somente permissão]	Concede permissão para descrever um administrador associado ao projeto	Read	project*		sso-directory:DescribeUsers sso:GetManagedApplicationInstance sso:ListProfileAssociations
ListProjectAdminUsers [somente permissão]	Concede permissão para listar todos os administradores associados ao projeto	Permissions management	project*		sso-directory:DescribeUsers sso:GetManagedApplicationInstance

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListProjectUserAssociations [somente permissão]	Concede permissão para listar todos os usuários associados ao projeto	Lista	project*		sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfileAssociations sso:ListProfiles
ListProjects [somente permissão]	Concede permissão para listar todos os projetos	List			
ListTagsForResource [somente permissão]	Concede permissão para listar todas as etiquetas de um recurso	Read	project		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListUserAccessRoleAssociations [somente permissão]	Concede permissão para listar todos os perfis de acesso associados ao usuário	Lista	project*		
TagResource [somente permissão]	Concede permissão para marcar um recurso	Marcação	project		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [somente permissão]	Concede permissão para desmarcar um recurso	Marcação	project		
				aws:TagKeys	
UpdateProject [somente permissão]	Concede permissão para atualizar um projeto	Write	project*		

Tipos de recursos definidos pelo Amazon Monitron

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
project	`arn:${Partition}:monitron:${Region}:${Account}:project/${ResourceId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o Amazon Monitron

O Amazon Monitron define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma IAM política. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso pelos pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas anexadas ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon MQ

O Amazon MQ (prefixo do serviço: `mq`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.

- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon MQ
- Tipos de recursos definidos pelo Amazon MQ
- Chaves de condição do Amazon MQ

Ações definidas pelo Amazon MQ

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateBroker	Concede permissão para criar um agente	Gravação		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateSecurityGroup ec2:CreateVpcEndpoint ec2:DescribeInternetGateways

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DescribeNetworkInterfacePermissions ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyNetworkInterfaceAttribute iam:CreateServiceLinkedRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					route53:AssociateVPCWithHostedZone
CreateConfiguration	Concede permissão para criar uma nova configuração para o nome da configuração especificada. O Amazon MQ usa a configuração padrão (o tipo e a versão do mecanismo)	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateReplicaBroker [somente permissão]	Concede permissão para criar um agente de réplicas	Gravar	brokers*		
CreateTags	Concede permissão para criar etiquetas	Marcação	brokers		
			configurations		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUser	Concede permissão para criar um usuário do ActiveMQ	Gravação	brokers*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteBroker	Concede permissão para excluir um agente	Gravar	brokers*		ec2:DeleteNetworkInterface ec2:DeleteNetworkInterfacePermission ec2:DeleteVpcEndpoints ec2:DetachNetworkInterface
DeleteConfiguration	Concede permissão para excluir uma configuração	Gravar	configurations*		
DeleteTags	Concede permissão para excluir etiquetas	Marcação	brokers		
			configurations		
				aws:TagKeys	
DeleteUser	Concede permissão para excluir um usuário do ActiveMQ	Gravação	brokers*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeBroker	Concede permissão para retornar informações sobre o agente especificado	Leitura	brokers*		
DescribeBrokerEngineTypes	Concede permissão para retornar informações sobre os mecanismos do agente	Leitura			
DescribeBrokerInstanceOptions	Concede permissão para retornar informações sobre as opções de instância de agente	Leitura			
DescribeConfiguration	Concede permissão para retornar informações sobre a configuração especificada	Leitura	configurations*		
DescribeConfigurationRevision	Concede permissão para retornar a revisão da configuração especificada para a configuração especificada	Leitura	configurations*		
DescribeUser	Concede permissão para retornar informações sobre o usuário do ActiveMQ	Leitura	brokers*		
ListBrokers	Concede permissão para retornar uma lista de todos os agentes	Listar			
ListConfigurationRevisions	Concede permissão para retornar uma lista de todas as revisões existentes da configuração especificada	Listar	configurations*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListConfigurations	Concede permissão para retornar uma lista de todas as configurações	Listar			
ListTags	Concede permissão para retornar uma lista de etiquetas	Listar	brokers		
			configurations		
ListUsers	Concede permissão para retornar uma lista de todos os usuários do ActiveMQ	Lista	brokers*		
Promote	Concede permissão para promover um agente	Gravar	brokers*		
RebootBroker	Concede permissão para reinicializar um agente	Gravação	brokers*		
UpdateBroker	Concede permissão para adicionar uma alteração de configuração pendente a um agente	Gravação	brokers*		
UpdateConfiguration	Concede permissão para atualizar a configuração especificada	Gravação	configurations*		
UpdateUser	Concede permissão para atualizar as informações de um usuário do ActiveMQ	Gravação	brokers*		

Tipos de recursos definidos pelo Amazon MQ

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
brokers	`arn:${Partition}:mq:${Region}:${Account}:broker:${BrokerName}:${BrokerId}`	aws:ResourceTag/${TagKey}
configurations	`arn:${Partition}:mq:${Region}:${Account}:configuration:${ConfigurationId}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon MQ

O Amazon MQ define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para aprovação multipartidária

A aprovação multipartidária (prefixo do serviço:`mpa`) fornece os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela aprovação multipartidária
- Tipos de recursos definidos pela aprovação de várias partes
- Chaves de condição para aprovação multipartidária

Ações definidas pela aprovação multipartidária

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelSession	Concede permissão para cancelar uma sessão de aprovação	Gravar	session*		
				aws:ResourceTag/${TagKey} mpa:RequestedOperation mpa:ProtectedResourceAccount	
CreateApprovalTeam	Concede permissão para criar uma equipe de aprovação	Gravar	approval-team*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateIdentitySource	Concede permissão para criar uma fonte de identidade	Gravar	identity-source*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteIdentitySource	Concede permissão para excluir uma fonte de identidade	Gravar	identity-source*		
				aws:ResourceTag/${TagKey}	
DeleteInactiveApprovalTeamVersion	Concede permissão para excluir uma equipe de aprovação inativa	Gravar	approval-team*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy [somente permissão]	Concede permissão para excluir uma política de recurso	Gerenciamento de permissões			
GetApprovalTeam	Concede permissão para recuperar detalhes para uma equipe de aprovação	Leitura	approval-team*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
GetIdentitySource	Concede permissão para recuperar detalhes de uma fonte de identidade	Leitura	identity-source*		
				aws:ResourceTag/${TagKey}	
GetPolicyVersion	Concede permissão para recuperar detalhes de uma política	Leitura			
GetResourcePolicy	Concede permissão para recuperar detalhes de um recurso específico	Leitura			
GetSession	Concede permissão para recuperar detalhes de uma sessão de aprovação	Leitura	session*		
				aws:ResourceTag/${TagKey} mpa:RequestedOperation mpa:ProtectedResourceAccount	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListApprovalTeams	Concede permissão para listar equipes de aprovação	Lista			
ListIdentitySources	Concede permissão para listar fontes de identidade	Lista			
ListPolicies	Concede permissão para listar políticas	Lista			
ListPolicyVersions	Concede permissão para listar as versões das políticas	Lista			
ListResourcePolicies	Concede permissão para listar políticas para um recurso	Lista			
ListSessions	Concede permissão para listar sessões de aprovação	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	List			
PutResourcePolicy [somente permissão]	Concede permissão para criar ou atualizar políticas para um recurso	Gerenciamento de permissões			
StartActiveApprovalTeamDeletion	Concede permissão para iniciar o processo de exclusão para uma equipe de aprovação ativa	Gravar	approval-team*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartSession [somente permissão]	Concede permissão para iniciar uma sessão de aprovação	Gravar	session*		
				aws:ResourceTag/${TagKey} mpa:RequestedOperation mpa:ProtectedResourceAccount	
TagResource	Concede permissão para marcar um recurso	Marcação		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso	Tags		aws:ResourceTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateApprovalTeam	Concede permissão para atualizar a equipe de aprovação	Gravar	approval-team*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pela aprovação de várias partes

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
approval-team	`arn:${Partition}:mpa:${Region}:${Account}:approval-team/${ApprovalTeamId}`	aws:ResourceTag/${TagKey}
identity-source	`arn:${Partition}:mpa:${Region}:${Account}:identity-source/${IdentitySourceId}`	aws:ResourceTag/${TagKey}
session	`arn:${Partition}:mpa:${Region}:${Account}:session/${SessionId}`	aws:ResourceTag/${TagKey}

Chaves de condição para aprovação multipartidária

A aprovação de várias partes define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por um par de chave valor da etiqueta que é permitido na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso por um par de chave e valor da etiqueta de um recurso.	Segmento
aws:TagKeys	Filtra o acesso por uma lista de chaves da etiqueta que são permitidas na solicitação	ArrayOfString
mpa:ProtectedResourceAccount	Filtra o acesso pela conta proprietária do recurso que é o alvo da operação que requer aprovação	String
mpa:RequestedOperation	Filtra o acesso por uma operação solicitada que requer aprovação da equipe antes de ser executada	String

Ações, recursos e chaves de condição do Amazon Neptune

O Amazon Neptune (prefixo do serviço: `neptune-db`) fornece os seguintes recursos, ações e chaves de contexto de condição para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.

- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Neptune
- Tipos de recursos definidos pelo Amazon Neptune
- Chaves de condição do Amazon Neptune

Ações definidas pelo Amazon Neptune

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelLoaderJob	Concede permissão para cancelar um trabalho de carregador	Gravar	database*		
CancelMLDataProcessingJob	Concede permissão para cancelar um trabalho de processamento de dados de ML	Gravar	database*		
CancelMLModelTrainingJob	Concede permissão para cancelar um trabalho de treinamento de modelo de ML	Gravar	database*		
CancelMLModelTransformJob	Concede permissão para cancelar um trabalho de transformação de modelo de ML	Gravar	database*		
CancelQuery	Concede permissão para cancelar uma consulta	Gravar	database*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateMLEndpoint	Concede permissão para criar um endpoint de ML	Gravar	database*		
DeleteDataViaQuery	Concede permissão para executar a exclusão de dados por meio de consulta APIs no banco de dados	Gravar	database*		
				neptune-db:QueryLanguage	
DeleteMLEndpoint	Concede permissão para excluir um endpoint de ML	Gravar	database*		
DeleteStatistics	Concede permissão para excluir todas as estatísticas do banco de dados	Gravar	database*		
GetEngineStatus	Concede permissão para verificar o status do mecanismo do Neptune	Leitura	database*		
GetGraphSummary	Concede permissão para obter o resumo em grafos com base no banco de dados	Leitura	database*		
GetLoaderJobStatus	Concede permissão para verificar o status de um trabalho de carregador	Leitura	database*		
GetMLDataProcessingJobStatus	Concede permissão para verificar o status de um trabalho de processamento de dados de ML	Leitura	database*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetMLEndpointStatus	Concede permissão para verificar o status de um endpoint de ML	Leitura	database*		
GetMLModelTrainingJobStatus	Concede permissão para verificar o status de um trabalho de modelo de treinamento de ML	Leitura	database*		
GetMLModelTransformJobStatus	Concede permissão para verificar o status de um trabalho de transformação de treinamento de ML	Leitura	database*		
GetQueryStatus	Concede permissão para verificar o status de todas as consultas ativas	Leitura	database*		
				neptune-db:QueryLanguage	
GetStatisticsStatus	Concede permissão para verificar o status das estatísticas do banco de dados	Leitura	database*		
GetStreamRecords	Concede permissão para buscar registros de fluxo do Neptune	Leitura	database*		
				neptune-db:QueryLanguage	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListLoaderJobs	Concede permissão para listar todos os trabalhos de carregador	Lista	database*		
ListMLDataProcessingJobs	Concede permissão para listar todos os trabalhos de processamento de dados de ML	Lista	database*		
ListMLEndpoints	Concede permissão para listar todos os endpoints de ML	Lista	database*		
ListMLModelTrainingJobs	Concede permissão para listar todos os trabalhos de treinamento de modelo de ML	Lista	database*		
ListMLModelTransformJobs	Concede permissão para listar todos os trabalhos de transformação de modelo de ML	Lista	database*		
ManageStatistics	Concede permissão para gerenciar estatísticas do banco de dados	Gravar	database*		
ReadDataViaQuery	Concede permissão para executar dados de leitura por meio de consulta APIs no banco de dados	Leitura	database*		
				neptune-db:QueryLanguage	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ResetDatabase	Concede permissão para obter o token necessário para redefinir e redefine o banco de dados Neptune	Gravar	database*		
StartLoaderJob	Concede permissão para iniciar um trabalho de carregador	Gravar	database*		
StartMLDataProcessingJob	Concede permissão para iniciar um trabalho de processamento de dados de ML	Gravar	database*		
StartMLModelTrainingJob	Concede permissão para iniciar um trabalho de treinamento de modelo de ML	Gravar	database*		
StartMLModelTransformJob	Concede permissão para iniciar um trabalho de transformação de modelo de ML	Gravar	database*		
WriteDataViaQuery	Concede permissão para executar dados de gravação por meio de consulta APIs no banco de dados	Gravar	database*		
				neptune-db:QueryLanguage	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
connect	Concede permissão para todas as ações de acesso a dados nas versões do mecanismo anteriores à versão 1.2.0.0	Gravar	database*		

Tipos de recursos definidos pelo Amazon Neptune

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
database	`arn:${Partition}:neptune-db:${Region}:${Account}:${ClusterResourceId}/*`	

Chaves de condição do Amazon Neptune

O Amazon Neptune define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
neptune-db:QueryLanguage	Filtra o acesso por modelo de grafo	String

Ações, recursos e chaves de condição do Amazon Neptune Analytics

O Amazon Neptune Analytics (prefixo do serviço: `neptune-graph`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Neptune Analytics
- Tipos de recursos definidos pelo Amazon Neptune Analytics
- Chaves de condição do Amazon Neptune Analytics

Ações definidas pelo Amazon Neptune Analytics

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o

nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

> **Note**
>
> Todas as ações do IAM, exceto ReadDataViaQuery '', WriteDataViaQuery 'e' DeleteDataViaQuery ', têm uma operação de API correspondente

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelExportTask	Concede permissão para cancelar uma tarefa de exportação em andamento	Gravar	export-task*		
				aws:ResourceTag/${TagKey}	
CancelImportTask	Concede permissão para cancelar uma tarefa de importação em andamento	Gravar	import-task*		
CancelQuery	Concede permissão para cancelar uma consulta	Gravar	graph*		
				aws:ResourceTag/${TagKey}	
CreateGraph	Concede permissão para criar um novo gráfico	Gravar	graph*		iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey
				aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys neptune-graph:PublicConnectivity	
CreateGraphSnapshot	Concede permissão para criar um novo snapshot a partir de um gráfico existente	Gravar	graph* graph-snapshot*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateGraphUsingImportTask	Concede permissão para criar um novo gráfico ao importar dados para o novo gráfico	Gravar	graph*		iam:CreateServiceLinkedRole iam:PassRole kms:CreateGrant kms:Decrypt kms:DescribeKey
			import-task*		
				aws:RequestTag/${TagKey} aws:TagKeys neptune-graph:PublicConnectivity	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreatePrivateGraphEndpoint	Concede permissão para criar um novo endpoint gráfico privado para acessar o gráfico de dentro de uma vpc	Gravar	graph*		ec2:CreateVpcEndpoint ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint route53:AssociateV

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					PCWithHostedZone
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteDataViaQuery	Concede permissão para excluir dados por meio de consulta APIs no gráfico	Gravar	graph*		
				aws:ResourceTag/${TagKey}	
DeleteGraph	Concede permissão para excluir um gráfico	Gravar	graph*		
				aws:ResourceTag/${TagKey}	
DeleteGraphSnapshot	Concede permissão para excluir um snapshot	Gravar	graph-snapshot*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeletePrivateGraphEndpoint	Concede permissão para excluir um endpoint de gráfico privado de um gráfico	Gravar	graph*		ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint route53:Disassocia

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					teVPCFromHostedZone
				aws:ResourceTag/${TagKey}	
GetEngineStatus	Concede permissão para obter o status do mecanismo de um gráfico	Leitura	graph*		
				aws:ResourceTag/${TagKey}	
GetExportTask	Concede permissão para obter detalhes sobre uma tarefa de exportação	Leitura	export-task*		
				aws:ResourceTag/${TagKey}	
GetGraph	Concede permissão para obter detalhes sobre um gráfico	Leitura	graph*		
				aws:ResourceTag/${TagKey}	
GetGraphSnapshot	Concede permissão para obter detalhes sobre um snapshot	Leitura	graph-snapshot*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetGraphSummary	Concede permissão para obter o resumo para os dados no gráfico	Leitura	graph*		
				aws:ResourceTag/${TagKey}	
GetImportTask	Concede permissão para obter detalhes sobre uma tarefa de importação	Leitura	import-task*		
GetPrivateGraphEndpoint	Concede permissão para obter detalhes sobre um endpoint de gráfico privado de um gráfico	Leitura	graph*		
				aws:ResourceTag/${TagKey}	
GetQueryStatus	Concede permissão para verificar o status de determinada consulta	Leitura	graph*		
				aws:ResourceTag/${TagKey}	
GetStatisticsStatus	Concede permissão para obter as estatísticas dos dados no gráfico	Leitura	graph*		
				aws:ResourceTag/${TagKey}	
ListExportTasks	Concede permissão para listar as tarefas de exportação em sua conta	Leitura	export-task*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListGraphSnapshots	Concede permissão para listar os snapshots na sua conta	Leitura	graph-snapshot*		
ListGraphs	Concede permissão para listar os gráficos na sua conta	Leitura	graph*		
ListImportTasks	Concede permissão para listar as tarefas de importação na sua conta	Leitura	import-task*		
ListPrivateGraphEndpoints	Concede permissão para listar os endpoints de gráficos privados para um determinado gráfico	Leitura	graph*		
				aws:ResourceTag/${TagKey}	
ListQueries	Concede permissão para verificar o status de todas as consultas ativas	Leitura	graph*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource	Concede permissão para listar tags para um recurso do Neptune Analytics	Leitura	graph		
			graph-snapshot		
				aws:ResourceTag/${TagKey}	
ReadDataViaQuery		Leitura	graph*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	Concede permissão para ler dados por meio de consulta APIs no gráfico			aws:ResourceTag/${TagKey}	
ResetGraph	Concede permissão para redefinir um gráfico que exclui todos os dados dentro do gráfico	Gravar	graph*		
				aws:ResourceTag/${TagKey}	
RestoreGraphFromSnapshot	Concede permissão para criar um novo gráfico a partir de um snapshot existente	Gravar	graph*		kms:CreateGrant kms:Decrypt kms:DescribeKey
			graph-snapshot*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys neptune-graph:PublicConnectivity	
StartExportTask	Concede permissão para exportar dados de um gráfico existente	Gravar	export-task* graph*		iam:PassRole
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartImportTask	Concede permissão para importar dados para um gráfico existente	Gravar	graph*		iam:PassRole
			import-task*		
TagResource	Concede permissão para atribuir tags a um recurso do Neptune Analytics	Tags	graph		
			graph-snapshot		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover tags de um recurso do Neptune Analytics	Tags	graph		
			graph-snapshot		
				aws:TagKeys	
UpdateGraph	Concede permissão para modificar um gráfico	Gravar	graph*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} neptune-graph:PublicConnectivity	
WriteDataViaQuery	Concede permissão para gravar dados por meio de consulta APIs no gráfico	Gravar	graph*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pelo Amazon Neptune Analytics

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
graph	`arn:${Partition}:neptune-graph:${Region}:${Account}:graph/${ResourceId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
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}`	

Chaves de condição do Amazon Neptune Analytics

O Amazon Neptune Analytics define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso pela chave e valor de uma etiqueta em uma solicitação	String
aws:ResourceTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta em uma solicitação	ArrayOfString

Chaves de condição	Descrição	Type
neptune-graph:PublicConnectivity	Filtra o acesso pelo valor do parâmetro de conectividade pública fornecido na solicitação ou seu valor padrão, se não for especificado. Todo o acesso aos gráficos é autenticado pelo IAM	Bool

Ações, recursos e chaves de condição do AWS Network Firewall

AWS O Network Firewall (prefixo do serviço:`network-firewall`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Network Firewall
- Tipos de recursos definidos pelo AWS Network Firewall
- Chaves de condição para o AWS Network Firewall

Ações definidas pelo AWS Network Firewall

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o

nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptNetworkFirewallTransi	Concede permissão para aceitar anexos pendentes	Gravar	Firewall*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
tGatewayAttachment	do Firewall de Rede em um gateway de trânsito				
AssociateAvailabilityZones	Concede permissão para associar zonas de disponibilidade a um firewall	Gravar	Firewall*		
AssociateFirewallPolicy	Concede permissão para criar uma associação entre uma política de firewall e um firewall	Write	Firewall*		
			FirewallPolicy*		
AssociateSubnets	Concede permissão para associar sub-redes VPC a um firewall	Gravar	Firewall*		
CreateFirewall	Concede permissão para criar um firewall de Firewall de AWS Rede	Gravar	Firewall*		iam:CreateServiceLinkedRole
			FirewallPolicy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFirewallPolicy	Concede permissão para criar uma política de firewall do Firewall de AWS Rede	Gravar	FirewallPolicy*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleGroup	Concede permissão para criar um grupo de regras do Firewall de AWS Rede	Gravar	StatefulRuleGroup		
			StatelessRuleGroup		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTLSInspectionConfiguration	Concede permissão para criar uma configuração de inspeção tls do Firewall de AWS Rede	Gravar	TLSInspectionConfiguration*		iam:CreateServiceLinkedRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVpcEndpointAssociation	Concede permissão para criar uma associação de endpoint vpc do AWS Network Firewall	Gravar	Firewall*		iam:CreateServiceLinkedRole
			VpcEndpointAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFirewall	Concede permissão para excluir um firewall	Write	Firewall*		
DeleteFirewallPolicy	Concede permissão para excluir uma política de firewall	Gravar	FirewallPolicy*		
DeleteNetworkFirewallTransitGatewayAttachment	Concede permissão para excluir anexos do Firewall de Rede em um gateway de trânsito	Gravar	Firewall*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteResourcePolicy	Concede permissão para excluir uma política de recursos para uma política de firewall, grupo de regras ou firewall	Gravar	Firewall		
			FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		
DeleteRuleGroup	Concede permissão para excluir um grupo de regras	Gravar	StatefulRuleGroup*		
			StatelessRuleGroup*		
DeleteTLSInspectionConfiguration	Concede permissão para excluir uma configuração de inspeção TLS	Gravar	TLSInspectionConfiguration*		
DeleteVpcEndpointAssociation	Concede permissão para excluir uma associação de endpoint vpc	Gravar	VpcEndpointAssociation*		
DescribeFirewall	Concede permissão para recuperar os objetos de dados que definem um firewall	Leitura	Firewall*		
DescribeFirewallMetadata	Concede permissão para recuperar as informações de alto nível sobre um firewall	Leitura	Firewall*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeFirewallPolicy	Concede permissão para recuperar os objetos de dados que definem uma política de firewall	Leitura	FirewallPolicy*		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
DescribeFlowOperation	Concede permissão para descrever uma operação de fluxo executada em um firewall	Leitura	Firewall*		
DescribeLoggingConfiguration	Concede permissão para descrever a configuração de log de um firewall	Leitura	Firewall*		logs:GetLogDelivery logs:ListLogDeliveries
DescribeResourcePolicy	Concede permissão para descrever uma política de recursos para uma política de firewall, um grupo de regras ou um firewall	Leitura	Firewall		
			FirewallPolicy		
			StatefulRuleGroup		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			Stateless RuleGroup		
DescribeRuleGroup	Concede permissão para recuperar os objetos de dados que definem um grupo de regras	Leitura	StatefulRuleGroup		
			Stateless RuleGroup		
DescribeRuleGroupMetadata	Concede permissão para recuperar as informações de alto nível sobre um grupo de regras	Leitura	StatefulRuleGroup		
			Stateless RuleGroup		
DescribeRuleGroupSummary	Concede permissão para recuperar as informações resumidas sobre um grupo de regras	Leitura	StatefulRuleGroup		
			Stateless RuleGroup		
DescribeTLSInspectionConfiguration	Concede permissão para recuperar os objetos de dados que definem uma configuração de inspeção TLS	Leitura	TLSInspectionConfiguration*		
DescribeVpcEndpointAssociation	Concede permissão para recuperar os objetos de dados que definem uma associação de endpoint vpc	Leitura	VpcEndpointAssociation*		
DisassociateAvailabilityZones	Concede permissão para desassociar zonas de disponibilidade de um firewall	Gravar	Firewall*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateSubnets	Concede permissão para desassociar sub-redes VPC de um firewall	Gravar	Firewall*		
GetAnalysisReportResults	Concede permissão para recuperar os resultados do relatório de análise de um firewall	Leitura	Firewall*		
ListAnalysisReports	Concede permissão para listar relatórios de análise de firewall	Lista	Firewall*		
ListFirewallPolicies	Concede permissão para recuperar os metadados das políticas de firewall	List	FirewallPolicy*		
ListFirewalls	Concede permissão para recuperar os metadados para firewalls	Lista	Firewall*		
ListFlowOperationResults	Concede permissão para listar os resultados de uma operação de fluxo executada em um firewall	Leitura	Firewall*		
ListFlowOperations	Concede permissão para listar as operações de fluxo realizadas em um firewall	Lista	Firewall*		
ListRuleGroups	Concede permissão para recuperar os metadados para grupos de regras	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTLSInspectionConfigurations	Concede permissão para recuperar os metadados para configurações de inspeção TLS	Lista	TLSInspectionConfiguration*		
ListTagsForResource	Concede permissão para recuperar as etiquetas de um recurso	Lista	Firewall*		
			FirewallPolicy*		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
			VpcEndpointAssociation		
ListVpcEndpointAssociations	Concede permissão para recuperar os metadados para associações de endpoints vpc	Lista	VpcEndpointAssociation*		
PutResourcePolicy	Concede permissão para colocar uma política de recursos para uma política de firewall, grupo de regras ou firewall	Gravar	Firewall		
			FirewallPolicy		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			StatefulRuleGroup		
			StatelessRuleGroup		
RejectNetworkFirewallTransitGatewayAttachment	Concede permissão para rejeitar anexos pendentes do Firewall de Rede em um gateway de trânsito	Gravar	Firewall*		
StartAnalysisReport	Concede permissão para iniciar um relatório de análise em um firewall	Gravar	Firewall*		
StartFlowCapture	Concede permissão para iniciar a operação de captura em um firewall	Gravar	Firewall*		
StartFlowFlush	Concede permissão para iniciar a operação de descarga em um firewall	Gravar	Firewall*		
TagResource	Concede permissão para anexar etiquetas a um recurso	Marcação	Firewall		
			FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			TLSInspectionConfiguration		
			VpcEndpointAssociation		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover etiquetas de um recurso	Tags	Firewall		
			FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
			VpcEndpointAssociation		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
UpdateAvailabilityZoneChangeProtection	Concede permissão para adicionar ou remover a proteção contra alteração da zona de disponibilidade de um firewall	Gravar	Firewall*		
UpdateFirewallAnalysisSettings	Concede permissão para modificar as configurações de análise de firewall de um firewall	Gravar	Firewall*		
UpdateFirewallDeleteProtection	Concede permissão para adicionar ou remover proteção de exclusão de um firewall	Write	Firewall*		
UpdateFirewallDescription	Concede permissão para modificar a descrição de um firewall	Gravar	Firewall*		
UpdateFirewallEncryptionConfiguration	Concede permissão para modificar a configuração de criptografia de um firewall	Gravar	Firewall*		
UpdateFirewallPolicy	Concede permissão para modificar uma política de firewall	Write	FirewallPolicy*		
			StatefulRuleGroup		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			Stateless RuleGroup		
			TLSInspectionConfiguration		
UpdateFirewallPolicyChangeProtection	Concede permissão para adicionar ou remover proteção contra alterações de política de firewall para um firewall	Write	Firewall*		
UpdateLoggingConfiguration	Concede permissão para modificar a configuração de log de um firewall	Write	Firewall*		
UpdateRuleGroup	Concede permissão para modificar um grupo de regras	Write	StatefulRuleGroup		
			Stateless RuleGroup		
UpdateSubnetChangeProtection	Concede permissão para adicionar ou remover proteção contra alteração de sub-rede para um firewall	Gravar	Firewall*		
UpdateTLSInspectionConfiguration	Concede permissão para modificar uma configuração de inspeção TLS	Gravar	TLSInspectionConfiguration*		

Tipos de recursos definidos pelo AWS Network Firewall

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
Firewall	`arn:${Partition}:network-firewall:${Region}:${Account}:firewall/${Name}`	aws:ResourceTag/${TagKey}
FirewallPolicy	`arn:${Partition}:network-firewall:${Region}:${Account}:firewall-policy/${Name}`	aws:ResourceTag/${TagKey}
StatefulRuleGroup	`arn:${Partition}:network-firewall:${Region}:${Account}:stateful-rulegroup/${Name}`	aws:ResourceTag/${TagKey}
StatelessRuleGroup	`arn:${Partition}:network-firewall:${Region}:${Account}:stateless-rulegroup/${Name}`	aws:ResourceTag/${TagKey}
TLSInspectionConfiguration	`arn:${Partition}:network-firewall:${Region}:${Account}:tls-configuration/${Name}`	aws:ResourceTag/${TagKey}
VpcEndpointAssociation	`arn:${Partition}:network-firewall:${Region}:${Account}:vpc-endpoint-association/${Name}`	aws:ResourceTag/${TagKey}

Chaves de condição para o AWS Network Firewall

AWS O Network Firewall define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelo conjunto de valores permitido para cada uma das etiquetas	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelo valor de etiqueta associado ao recurso	String
aws:TagKeys	Filtra o acesso pela presença de etiquetas obrigatórias na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o Network Flow Monitor

O Network Flow Monitor (prefixo do serviço:`networkflowmonitor`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Network Flow Monitor

- Tipos de recursos definidos pelo Network Flow Monitor
- Chaves de condição para o Network Flow Monitor

Ações definidas pelo Network Flow Monitor

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateMonitor	Concede permissão para criar um monitor	Gravar	monitor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateScope	Concede permissão para criar um escopo	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteMonitor	Concede permissão para excluir um monitor	Gravar	monitor*		
DeleteScope	Concede permissão para excluir um escopo	Gravar	scope*		
GetMonitor	Concede permissão para obter informações sobre um monitor	Leitura	monitor*		
GetQueryResultsMon	Concede permissão para obter os resultados de uma	Leitura	monitor*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
itorTopContributors	consulta que recupera os dados dos principais colaboradores para um monitor				
GetQueryResultsWorkloadInsightsTopContributors	Concede permissão para obter os resultados de uma consulta que recupera os principais colaboradores para obter informações sobre a carga de trabalho	Leitura	scope*		
GetQueryResultsWorkloadInsightsTopContributorsData	Concede permissão para obter os resultados de uma consulta que recupera os pontos de dados dos principais colaboradores para obter informações sobre a carga de trabalho	Leitura	scope*		
GetQueryStatusMonitorTopContributors	Concede permissão para obter o status de uma consulta que recupera os dados dos principais colaboradores para um monitor	Leitura	monitor*		
GetQueryStatusWorkloadInsightsTopContributors	Concede permissão para obter o status de uma consulta que recupera os principais colaboradores para obter informações sobre a carga de trabalho	Leitura	scope*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetQueryStatusWorkloadInsightsTopContributorsData	Concede permissão para obter o status de uma consulta que recupera os pontos de dados dos principais colaboradores para obter informações sobre a carga de trabalho	Leitura	scope*		
GetScope	Concede permissão para obter informações sobre um escopo	Leitura	scope*		
ListMonitors	Concede permissão para listar todos os monitores em uma conta e seus status	Lista			
ListScopes	Concede permissão para obter todos os escopos de uma conta	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	monitor scope		
Publish	Concede permissão para publicar um relatório	Gravar			
StartQueryMonitorTopContributors	Concede permissão para iniciar uma consulta para recuperar os dados dos principais colaboradores para um monitor	Gravar	monitor*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartQueryWorkloadInsightsTopContributors	Concede permissão para iniciar uma consulta para recuperar os dados dos principais colaboradores para obter informações sobre a carga de trabalho	Gravar	scope*		
StartQueryWorkloadInsightsTopContributorsData	Concede permissão para iniciar uma consulta para recuperar pontos de dados dos principais colaboradores para obter informações sobre a carga de trabalho	Gravar	scope*		
StopQueryMonitorTopContributors	Concede permissão para interromper uma consulta para recuperar dados dos principais colaboradores para um monitor	Gravar	monitor*		
StopQueryWorkloadInsightsTopContributors	Concede permissão para interromper uma consulta para recuperar os principais colaboradores para obter informações sobre a carga de trabalho	Gravar	scope*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopQueryWorkloadInsightsTopContributorsData	Concede permissão para interromper uma consulta para recuperar pontos de dados dos principais colaboradores para obter informações sobre a carga de trabalho	Gravar	scope*		
TagResource	Concede permissão para adicionar tags a um recurso	Marcação	monitor		
			scope		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover etiquetas de um recurso	Tags	monitor		
			scope		
				aws:TagKeys	
UpdateMonitor	Concede permissão para atualizar um monitor	Gravar	monitor*		
UpdateScope	Concede permissão para atualizar um escopo	Gravar	scope*		

Tipos de recursos definidos pelo Network Flow Monitor

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
monitor	`arn:${Partition}:networkflowmonitor:${Region}:${Account}:monitor/${MonitorName}`	aws:ResourceTag/${TagKey}
scope	`arn:${Partition}:networkflowmonitor:${Region}:${Account}:scope/${ScopeId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o Network Flow Monitor

O Network Flow Monitor define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso pelos pares de chave-valor da etiqueta na solicitação	String

Chaves de condição	Descrição	Type
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS Network Manager

AWS O Network Manager (prefixo do serviço:`networkmanager`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Network Manager
- Tipos de recursos definidos pelo AWS Network Manager
- Chaves de condição para o AWS Network Manager

Ações definidas pelo AWS Network Manager

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptAttachment	Concede permissão para aceitar a criação de um anexo entre uma fonte e um destino em uma rede principal	Gravar	attachment*		ec2:DescribeRegions
AssociateConnectPeer	Concede permissão para associar um Connect Peer	Gravar	device*		
			global-network*		
AssociateCustomerGateway	Concede permissão para associar um gateway do cliente a um dispositivo	Write	device*		
			global-network*		
			link		
				networkmanager:cgwArn	
AssociateLink	Concede permissão para associar um link a um dispositivo	Write	device*		
			global-network*		
			link*		
AssociateTransitGatewayConnectPeer	Concede permissão para associar um par de conexão de gateway de trânsito a um dispositivo	Gravar	device*		
			global-network*		
			link		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				networkmanager:tgwConnectPeerArn	
CreateConnectAttachment	Concede permissão para criar um anexo do Connect	Gravar	attachment*		ec2:DescribeRegions networkmanager:TagResource
			core-network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnectPeer	Concede permissão para criar uma conexão Connect Peer	Gravar	attachment*		ec2:DescribeRegions networkmanager:TagResource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnection	Concede permissão para criar uma nova conexão	Gravar	global-network*		networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCoreNetwork	Concede permissão para criar uma nova rede principal	Gravar	global-network*		ec2:DescribeRegions networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDevice	Concede permissão para criar um novo dispositivo	Gravar	global-network*		networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDirectConnectGatewayAttachment	Concede permissão para criar um anexo de gateway Direct Connect	Gravar	core-network*		ec2:DescribeRegions networkmanager:TagResource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:directConnectGatewayArn networkmanager:edgeLocations	
CreateGlobalNetwork	Concede permissão para criar uma nova rede global	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole networkmanager:TagResource
CreateLink	Concede permissão para criar um novo link	Write	global-network*		networkmanager:TagResource
			site		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSite	Concede permissão para criar um novo site	Gravar	global-network*		networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSiteToSiteVpnAttachment	Concede permissão para criar um anexo de site-to-site VPN	Gravar	core-network*		ec2:DescribeRegions networkmanager:TagResource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:vpnConnectionArn	
CreateTransitGatewayPeering	Concede permissão para criar um emparelhamento do Transit Gateway	Gravar	core-network*		ec2:DescribeRegions networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:tgwArn	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateTransitGatewayRouteTableAttachment	Concede permissão para criar um anexo do TGW RTB	Gravar	peering*		ec2:DescribeRegions networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:tgwRtbArn	
CreateVpcAttachment	Concede permissão para criar um anexo do VPC	Gravar	core-network*		ec2:DescribeRegions networkmanager:TagResource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:vpcArn networkmanager:subnetArns	
DeleteAttachment	Concede permissão para excluir um anexo	Gravar	attachment*		ec2:DescribeRegions
DeleteConnectPeer	Concede permissão para excluir um Connect Peer	Gravar	connect-peer*		ec2:DescribeRegions
DeleteConnection	Concede permissão para excluir uma conexão	Gravar	connection*		
			global-network*		
DeleteCoreNetwork	Concede permissão para excluir uma rede principal	Gravar	core-network*		ec2:DescribeRegions

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteCoreNetworkPolicyVersion	Concede permissão para excluir a versão da política de rede principal	Gravar	core-network*		
DeleteDevice	Concede permissão para excluir um dispositivo	Write	device*		
			global-network*		
DeleteGlobalNetwork	Concede permissão para excluir uma rede global	Write	global-network*		
DeleteLink	Concede permissão para excluir um link	Gravar	global-network*		
			link*		
DeletePeering	Concede permissão para excluir um emparelhamento	Gravar	peering*		ec2:DescribeRegions
DeleteResourcePolicy	Concede permissão para excluir um recurso	Gravar	core-network*		
DeleteSite	Concede permissão para excluir um site	Write	global-network*		
			site*		
DeregisterTransitGateway	Concede permissão para cancelar o registro de um gateway de trânsito de uma rede global	Write	global-network*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				networkmanager:tgwArn	
DescribeGlobalNetworks	Concede permissão para descrever redes globais	Lista	global-network		
DisassociateConnectPeer	Concede permissão para desassociar um Connect Peer	Gravar	global-network*		
DisassociateCustomerGateway	Concede permissão para desassociar um gateway do cliente de um dispositivo	Write	global-network*		
				networkmanager:cgwArn	
DisassociateLink	Concede permissão para desassociar um link de um dispositivo	Write	device*		
			global-network*		
			link*		
DisassociateTransitGatewayConnectPeer	Concede permissão para desassociar um par de conexão de gateway de trânsito de um dispositivo	Gravar	global-network*		
				networkmanager:tgwConnectPeerArn	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ExecuteCoreNetworkChangeSet	Concede permissão para aplicar alterações à rede principal	Gravar	core-network*		ec2:DescribeRegions
GetConnectAttachment	Concede permissão para recuperar um anexo do Connect	Leitura	attachment*		
GetConnectPeer	Concede permissão para recuperar um Connect Peer	Leitura	connect-peer*		
GetConnectPeerAssociations	Concede permissão para descrever associações de Connect Peer	Leitura	global-network*		
GetConnections	Concede permissão para descrever conexões	Lista	global-network*		
			connection		
GetCoreNetwork	Concede permissão para recuperar uma rede principal	Leitura	core-network*		
GetCoreNetworkChangeEvents	Concede permissão para recuperar uma lista de eventos de alterações de rede principal	Leitura	core-network*		
GetCoreNetworkChangeSet	Concede permissão para recuperar uma lista de conjuntos de alterações de rede de núcleo	Leitura	core-network*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetCoreNetworkPolicy	Concede permissão para recuperar a política de rede principal	Leitura	core-network*		
GetCustomerGatewayAssociations	Concede permissão para descrever associações de gateway de clientes	List	global-network*		
GetDevices	Concede permissão para descrever dispositivos	Lista	global-network*		
			device		
GetDirectConnectGatewayAttachment	Concede permissão para recuperar um anexo do gateway Direct Connect	Leitura	attachment*		
GetLinkAssociations	Concede permissão para descrever associações de links	List	global-network*		
			device		
			link		
GetLinks	Concede permissão para descrever links	Lista	global-network*		
			link		
GetNetworkResourceCounts	Concede permissão para retornar o número de recursos para uma rede global agrupada por tipo	Leitura	global-network*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetNetworkResourceRelationships	Concede permissão para recuperar recursos relacionados para um recurso dentro da rede global	Leitura	global-network*		
GetNetworkResources	Concede permissão para recuperar um recurso de rede global	Leitura	global-network*		
GetNetworkRoutes	Concede permissão para recuperar rotas para uma tabela de rotas dentro da rede global	Leitura	global-network*		
GetNetworkTelemetry	Concede permissão para recuperar objetos de telemetria de rede para a rede global	Leitura	global-network*		
GetResourcePolicy	Concede permissão para recuperar uma política de recurso	Leitura	core-network*		
GetRouteAnalysis	Concede permissão para recuperar uma configuração de análise de rota e um resultado	Leitura	global-network*		
GetSiteToSiteVpnAttachment	Concede permissão para recuperar um anexo de site-to-site VPN	Leitura	attachment*		
GetSites	Concede permissão para descrever redes globais	List	global-network*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			site		
GetTransitGatewayConnectPeerAssociations	Concede permissão para descrever associações de pares de conexão de gateway de trânsito	Lista	global-network*		
GetTransitGatewayPeering	Concede permissão para recuperar um emparelhamento do Transit Gateway	Leitura	peering*		
GetTransitGatewayRegistrations	Concede permissão para descrever registros de gateway de trânsito	Lista	global-network*		
GetTransitGatewayRouteTableAttachment	Concede permissão para recuperar um anexo do TGW RTB	Leitura	attachment*		
GetVpcAttachment	Concede permissão para recuperar um anexo da VPC	Leitura	attachment*		
ListAttachments	Concede permissão para descrever anexos	Lista	attachment*		
ListConnectPeers	Concede permissão para descrever Connect Peers	Lista	connect-peer*		
ListCoreNetworkPolicyVersions	Concede permissão para listar versões de políticas de rede principal	Lista	core-network*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListCoreNetworks	Concede permissão para listar redes principais	Lista			
ListOrganizationServiceAccessStatus	Concede permissão para listar o status de acesso ao serviço da organização	Lista			
ListPeerings	Concede permissão para descrever emparelhamentos	Lista			
ListTagsForResource	Concede permissão para listar marcações para um recurso do Network Manager	Leitura	attachment		
			connect-peer		
			connection		
			core-network		
			device		
			global-network		
			link		
			peering		
			site		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
PutCoreNetworkPolicy	Concede permissão para criar uma política de rede principal	Gravar	core-network*		ec2:DescribeRegions
PutResourcePolicy	Concede permissão para criar ou atualizar uma política de recurso	Gravar	core-network*		
RegisterTransitGateway	Concede permissão para registrar um gateway de trânsito em uma rede global	Gravar	global-network*		
				networkmanager:tgwArn	
RejectAttachment	Concede permissão para rejeitar solicitação de anexo	Gravar	attachment*		
RestoreCoreNetworkPolicyVersion	Concede permissão para restaurar a política de rede principal para uma versão anterior	Gravar	core-network*		ec2:DescribeRegions
StartOrganizationServiceAccessUpdate	Concede permissão para iniciar a atualização do acesso ao serviço da organização	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartRouteAnalysis	Concede permissão para iniciar uma análise de rota e armazena a configuração de análise	Gravar	global-network*		
TagResource	Concede permissão para marcar um recurso do Gerenciador de rede	Marcação	attachment		
			connect-peer		
			connection		
			core-network		
			device		
			global-network		
			link		
			peering		
			site		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permissão para desmarcar um recurso do Gerenciador de rede	Marcação	attachment		
			connect-peer		
			connection		
			core-network		
			device		
			global-network		
			link		
			peering		
			site		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
UpdateConnection	Concede permissão para atualizar uma conexão	Gravar	connection*		
			global-network*		
UpdateCoreNetwork	Concede permissão para atualizar uma rede princpal	Gravar	core-network*		
UpdateDevice	Concede permissão para atualizar um dispositivo	Gravar	device*		
			global-network*		
UpdateDirectConnectGatewayAttachment	Concede permissão para atualizar um anexo do gateway Direct Connect	Gravar	attachment*		ec2:DescribeRegions
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:edgeLocations	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateGlobalNetwork	Concede permissão para atualizar uma rede global	Write	global-network*		
UpdateLink	Concede permissão para atualizar um link	Gravar	global-network*		
			link*		
UpdateNetworkResourceMetadata	Concede permissão para adicionar ou atualizar key/value pares de metadados no recurso de rede	Gravar	global-network*		
UpdateSite	Concede permissão para atualizar um site	Gravar	global-network*		
			site*		
UpdateVpcAttachment	Concede permissão para atualizar um anexo do VPC	Gravar	attachment*		ec2:DescribeRegions
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:subnetArns	

Tipos de recursos definidos pelo AWS Network Manager

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
peering	`arn:${Partition}:networkmanager::${Account}:peering/${ResourceId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o AWS Network Manager

AWS O Network Manager define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString
networkmanager:cgwArn	Controla o acesso por quais gateways do cliente podem ser associados ou desassociados	ARN
networkmanager:directConnectGatewayArn	Filtra o acesso pelo qual o gateway Direct Connect pode ser usado a um create/update anexo	ARN

Chaves de condição	Descrição	Tipo
networkmanager:edgeLocations	Filtra o acesso por meio do qual os pontos de presença podem ser adicionados ou removidos de um anexo do gateway Direct Connect	ArrayOfString
networkmanager:subnetArns	Filtra o acesso pelo qual as sub-redes VPC podem ser adicionadas ou removidas de um anexo VPC	ArrayOfARN
networkmanager:tgwArn	Filtra o acesso pelo qual gateways de trânsito podem ser registrados, ter o registro cancelado ou emparelhados	ARN
networkmanager:tgwConnectPeerArn	Filtra o acesso pelo qual pares de conexão do Transit Gateway podem ser associados ou desassociados	ARN
networkmanager:tgwRtbArn	Filtra o acesso pelo qual a tabela de rotas do Transit Gateway pode ser usada para criar um anexo	ARN
networkmanager:vpcArn	Filtra o acesso pelo qual a VPC pode ser usada em um anexo create/update	ARN
networkmanager:vpnConnectionArn	Filtra o acesso pelo qual a Site-to-Site VPN pode ser usada em um create/update anexo	ARN

Ações, recursos e chaves de condição para o AWS Network Manager Chat

AWS O Network Manager Chat (prefixo do serviço:`networkmanager-chat`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.

- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Network Manager Chat
- Tipos de recursos definidos pelo AWS Network Manager Chat
- Chaves de condição para o AWS Network Manager Chat

Ações definidas pelo AWS Network Manager Chat

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelMessageResponse [somente permissão]	Concede permissão para cancelar uma resposta a uma mensagem	Gravar			
CreateConversation [somente permissão]	Concede permissão para criar uma conversa	Gravar			
DeleteConversation [somente permissão]	Concede permissão para excluir uma conversa	Gravar			
ListConversationMessages [somente permissão]	Concede permissão para listar mensagens de conversas	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListConversations [somente permissão]	Concede permissão para listar conversas	Lista			
NotifyConversationIsActive [somente permissão]	Concede permissão para notificar se há atividade em uma conversa	Gravar			
SendConversationMessage [somente permissão]	Concede permissão para enviar uma mensagens de conversa	Gravar			

Tipos de recursos definidos pelo AWS Network Manager Chat

AWS O Network Manager Chat não suporta a especificação de um ARN de recurso no elemento de uma `Resource` declaração de política do IAM. Para permitir ao acesso ao AWS Network Manager Chat, especifique `"Resource": "*"` em sua política.

Chaves de condição para o AWS Network Manager Chat

O Network Manager Chat não possui chaves de contexto específicas do serviço que possam ser usadas no elemento `Condition` das instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do Amazon Nimble Studio

O Amazon Nimble Studio (prefixo de serviço: `nimble`) fornece os recursos, ações e chaves de contexto de condição específicos do serviço abaixo para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Nimble Studio
- Tipos de recurso definidos pelo Amazon Nimble Studio
- Chaves de condição do Amazon Nimble Studio

Ações definidas pelo Amazon Nimble Studio

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptEulas	Concede permissão para aceitar EULAs	Gravar	eula*		
CreateLaunchProfile	Concede permissão para criar um perfil de execução.	Write	studio*		ec2:CreateNetworkInterface ec2:DescribeNatGateways ec2:DescribeNetworkAcls

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DescribeRouteTables ec2:DescribeSubnets ec2:DescribeVpcEndpoints ec2:RunInstances
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateStreamingImage	Concede permissão para criar uma imagem de streaming.	Write	studio*		ec2:DescribeImages ec2:DescribeSnapshots ec2:ModifyInstanceAttribute ec2:ModifySnapshotAttribute ec2:RegisterImage
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateStreamingSession	Concede permissão para criar uma sessão de streaming.	Gravar	launch-profile*		ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission nimble:GetLaunchProfile nimble:GetLaunchProfileInitialization nimble:ListEulaAcceptances
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStreamingSessionStream	Concede permissão para criar um StreamingSessionStream	Gravar	streaming-session*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				nimble:requesterPrincipalId	
CreateStudio	Concede permissão para criar um estúdio.	Write	studio*		iam:PassRole sso:CreateManagedApplicationInstance
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateStudioComponent	Concede permissão para criar um componente de estúdio. Um componente de estúdio designa um recurso de rede ao qual um perfil de execução oferecerá acesso.	Write	studio*		ds:AuthorizeApplication ds:DescribeDirectories ec2:DescribeSecurityGroups fsx:DescribeFileSystems iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteLaunchProfile	Concede permissão para excluir um perfil de execução.	Write	launch-profile*		
DeleteLaunchProfileMember	Concede permissão para excluir um membro de um perfil de execução.	Write	launch-profile*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteStreamingImage	Concede permissão para excluir uma imagem de streaming.	Write	streaming-image*		ec2:DeleteSnapshot ec2:DeregisterImage ec2:ModifyInstanceAttribute ec2:ModifySnapshotAttribute
DeleteStreamingSession	Concede permissão para excluir uma sessão de streaming.	Write	streaming-session*		ec2:DeleteNetworkInterface
				nimble:requesterPrincipalId	
DeleteStudio	Concede permissão para excluir um estúdio.	Write	studio*		sso:DeleteManagedApplicationInstance
DeleteStudioComponent	Concede permissão para excluir um componente de estúdio.	Write	studio-component*		ds:UnauthorizeApplication

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteStudioMember	Concede permissão para excluir um membro de um estúdio.	Write	studio*		
GetEula	Concede permissão para obter um EULA.	Read	eula*		
GetFeatureMap [somente permissão]	Concede permissão para permitir que o portal do Nimble Studio mostre os recursos apropriados para a conta.	Read			
GetLaunchProfile	Concede permissão para obter um perfil de execução.	Read	launch-profile*		
GetLaunchProfileDetails	Concede permissão para obter os detalhes de um perfil de execução, que incluem o resumo dos componentes de estúdio e das imagens de streaming usadas pelo perfil de execução.	Read	launch-profile*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetLaunchProfileInitialization	Concede permissão para obter uma inicialização de perfil de execução. Uma inicialização é uma versão sem referência de um perfil de execução que inclui informações sobre a conexão associada ao componente de estúdio.	Read	launch-profile*		ds:DescribeDirectories ec2:DescribeSecurityGroups fsx:DescribeFileSystems
GetLaunchProfileMember	Concede permissão para obter um membro de um perfil de execução.	Read	launch-profile*		
GetStreamingImage	Concede permissão para obter uma imagem de streaming.	Read	streaming-image*		
GetStreamingSession	Concede permissão para obter uma sessão de streaming.	Leitura	streaming-session*		
				nimble:requesterPrincipalId	
GetStreamingSessionBackup	Concede permissão para obter um backup de sessão de streaming	Leitura	streaming-session-backup*		
				nimble:requesterPrincipalId	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetStreamingSessionStream	Concede permissão para obter um stream de uma sessão de streaming.	Read	streaming-session*		
				nimble:requesterPrincipalId	
GetStudio	Concede permissão para obter um estúdio.	Read	studio*		
GetStudioComponent	Concede permissão para obter um componente de estúdio.	Read	studio-component*		
GetStudioMember	Concede permissão para obter um membro de um estúdio.	Read	studio*		
ListEulaAcceptances	Concede permissão para listar as aceitações dos EULAs.	Leitura	eula-acceptance*		
ListEulas	Concede permissão para listar EULAs	Leitura	eula*		
ListLaunchProfileMembers	Concede permissão para listar os membros de um perfil de execução.	Read	launch-profile*		
ListLaunchProfiles	Concede permissão para listar perfis de execução.	Read	studio*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				nimble:principalId nimble:requesterPrincipalId	
ListStreamingImages	Concede permissão para listar imagens de streaming.	Leitura	studio*		
ListStreamingSessionBackups	Concede permissão para listar os backups de sessão de streaming	Leitura	studio*		
				nimble:requesterPrincipalId	
ListStreamingSessions	Concede permissão para listar sessões de streaming.	Read	studio*		
				nimble:createdBy nimble:ownedBy nimble:requesterPrincipalId	
ListStudioComponents	Concede permissão para listar componentes de estúdio.	Read	studio*		
ListStudioMembers	Concede permissão para listar os membros de um estúdio.	Read	studio*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListStudios	Concede permissão para listar todos os estúdios.	Read			
ListTagsForResource	Concede permissão para listar todas as etiquetas de um recurso do Nimble Studio.	Leitura	launch-profile		
			streaming-image		
			streaming-session		
			streaming-session-backup		
			studio		
			studio-component		
PutLaunchProfileMembers	Concede permissão para add/update lançar membros do perfil	Gravar	launch-profile*		sso-directory:DescribeUsers
PutStudioLogEvents [somente permissão]	Concede permissão para relatar métricas e logs do portal do Nimble Studio para monitorar a integridade da aplicação.	Gravar	studio*		
PutStudioMembers	Concede permissão aos membros do add/update estúdio	Gravar	studio*		sso-directory:DescribeUsers

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartStreamingSession	Concede permissão para iniciar uma sessão de transmissão	Gravar	streaming-session*		nimble:GetLaunchProfile nimble:GetLaunchProfileMember
			streaming-session-backup		
				nimble:requesterPrincipalId	
StartStudioSSOConfigurationRepair	Concede permissão para reparar a configuração do AWS IAM Identity Center do estúdio	Gravar	studio*		sso:CreateManagedApplicationInstance sso:GetManagedApplicationInstance
StopStreamingSession	Concede permissão para interromper uma sessão transmissão	Gravar	streaming-session*		nimble:GetLaunchProfile

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				nimble:requesterPrincipalId	
TagResource	Concede permissão para adicionar ou substituir uma ou mais etiquetas do recurso especificado do Nimble Studio.	Marcação	launch-profile		
			streaming-image		
			streaming-session		
			streaming-session-backup		
			studio		
			studio-component		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para desassociar uma ou mais etiquetas do recurso especificado do Nimble Studio.	Marcação	launch-profile		
			streaming-image		
			streaming-session		
			streaming-session-backup		
			studio		
			studio-component		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateLaunchProfile	Concede permissão para atualizar um perfil de execução.	Write	launch-profile*		ec2:DescribeNatGateways ec2:DescribeNetworkAcls ec2:DescribeRouteTables ec2:DescribeSubnets ec2:DescribeVpcEndpoints
UpdateLaunchProfileMember	Concede permissão para atualizar um membro de um perfil de execução.	Write	launch-profile*		
UpdateStreamingImage	Concede permissão para atualizar uma imagem de streaming.	Write	streaming-image*		
UpdateStudio	Concede permissão para atualizar um estúdio.	Write	studio*		iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateStudioComponent	Concede permissão para atualizar um componente de estúdio.	Write	studio-component*		ds:AuthorizeApplication ds:DescribeDirectories ec2:DescribeSecurityGroups fsx:DescribeFileSystems iam:PassRole

Tipos de recurso definidos pelo Amazon Nimble Studio

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
studio	`arn:${Partition}:nimble:${Region}:${Account}:studio/${StudioId}`	aws:RequestTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
		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 recursos	ARN	Chaves de condição
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

Chaves de condição do Amazon Nimble Studio

O Amazon Nimble Studio define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por um par de chave valor da etiqueta que é permitido na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso por um par de chave e valor da etiqueta de um recurso.	Segmento
aws:TagKeys	Filtra o acesso por uma lista de chaves da etiqueta que são permitidas na solicitação	ArrayOfString
nimble:createdBy	Filtra o acesso pelo parâmetro de solicitação createdBy ou no ID do criador do recurso	String
nimble:ownedBy	Filtra o acesso pelo parâmetro de solicitação ownedBy ou no ID do proprietário do recurso	String
nimble:principalId	Filtra o acesso pelo parâmetro de solicitação principalId	String
nimble:requesterPrincipalId	Filtra o acesso pela ID do usuário conectado	String
nimble:studioId	Filtra o acesso por um studio específico	ARN

Ações, recursos e chaves de condição do Amazon One Enterprise

O Amazon One Enterprise (prefixo do serviço: one) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissões do IAM.

Referências:

- Saiba como configurar este serviço.

- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon One Enterprise
- Tipos de recursos definidos pelo Amazon One Enterprise
- Chaves de condição do Amazon One Enterprise

Ações definidas pelo Amazon One Enterprise

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDeviceActivationQrCode	Concede permissão para criar um código QR para uma instância de dispositivo	Gravar	device-instance*		
				aws:ResourceTag/${TagKey}	
CreateDeviceConfigurationTemplate	Concede permissão para criar um modelo de configuração de dispositivo	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeviceInstance	Concede permissão para criar uma instância de dispositivo	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDeviceInstanceConfiguration	Concede permissão para criar uma configuração de instância de dispositivo	Gravar	device-instance*		
				aws:ResourceTag/${TagKey}	
CreateSite	Concede permissão para criar um site	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAssociatedDevice	Concede permissão para desassociar um dispositivo de uma instância de dispositivo	Gravar	device-instance*		
				aws:ResourceTag/${TagKey}	
DeleteDeviceConfigurationTemplate	Concede permissão para excluir um modelo de configuração de dispositivo	Gravar	device-configuration-template*		
				aws:ResourceTag/${TagKey}	
DeleteDeviceInstance	Concede permissão para excluir uma instância de dispositivo	Gravar	device-instance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
DeleteSite	Concede permissão para excluir um site	Gravar	site*		
				aws:ResourceTag/${TagKey}	
DeleteUserV1	Concede permissão para excluir um usuário	Gravar	user*		
GetDeviceConfigurationTemplate	Concede permissão para visualizar um modelo de configuração de dispositivo	Leitura	device-configuration-template*		
				aws:ResourceTag/${TagKey}	
GetDeviceInstance	Concede permissão para visualizar uma instância de dispositivo	Leitura	device-instance*		
				aws:ResourceTag/${TagKey}	
GetDeviceInstanceConfiguration	Concede permissão para visualizar uma configuração de instância de dispositivo	Leitura	configuration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
GetSite	Concede permissão para visualizar um site	Leitura	site*		
				aws:ResourceTag/${TagKey}	
GetSiteAddress	Concede permissão para visualizar o endereço de um site	Leitura	site*		
				aws:ResourceTag/${TagKey}	
ListDeviceConfigurationTemplates	Concede permissão para recuperar a lista de modelos de configuração do dispositivo	Lista			
ListDeviceInstances	Concede permissão para recuperar a lista de instâncias de dispositivos	Lista			
ListSites	Concede permissão para visualizar a lista de sites	Lista			
ListTagsForResource	Concede permissão para listar tags para um recurso do Amazon One Enterprise	Leitura	device-configuration-template		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			device-instance		
			site		
				aws:ResourceTag/${TagKey}	
ListUsersV1	Concede permissão para visualizar a lista de usuários	Lista			
RebootDevice	Concede permissão para reinicializar o dispositivo associado a uma instância de dispositivo	Gravar	device-instance*		
				aws:ResourceTag/${TagKey}	
TagResource	Concede permissão para adicionar tags a um recurso do Amazon One Enterprise	Tags	device-configuration-template		
			device-instance		
			site		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover tags de um recurso do Amazon One Enterprise	Tags	device-configuration-template		
			device-instance		
			site		
				aws:TagKeys	
UpdateDeviceConfigurationTemplate	Concede permissão para atualizar um modelo de configuração de dispositivo	Gravar	device-configuration-template*		
				aws:ResourceTag/${TagKey}	
UpdateDeviceInstance	Concede permissão para atualizar uma instância de dispositivo	Gravar	device-instance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
UpdateSite	Concede permissão para atualizar um site	Gravar	site*		
				aws:ResourceTag/${TagKey}	
UpdateSiteAddress	Concede permissão para atualizar o endereço de um site	Gravar	site*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pelo Amazon One Enterprise

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
device-instance	`arn:${Partition}:one:${Region}:${Account}:device-instance/${DeviceInstanceId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
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}`	

Chaves de condição do Amazon One Enterprise

O Amazon One Enterprise define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso usando pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso usando pares de chave-valor da etiqueta anexados ao recurso	String

Chaves de condição	Descrição	Tipo
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para a Amazon OpenSearch

A Amazon OpenSearch (prefixo do serviço:`opensearch`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon OpenSearch
- Tipos de recursos definidos pela Amazon OpenSearch
- Chaves de condição para a Amazon OpenSearch

Ações definidas pela Amazon OpenSearch

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ApplicationAccessAll [somente permissão]	Concede permissão para acessar o OpenSearch Aplicativo	Gerenciamento de permissões	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelDirectQuery	Concede permissão para cancelar a consulta enviada no OpenSearch DataSource recurso	Gravar	datasource*		
GetDirectQuery	Concede permissão para obter o status da consulta que é executada no OpenSearch DataSource recurso	Leitura	datasource*		
GetDirectQueryResult	Concede permissão para obter os resultados de uma consulta que é executada no OpenSearch DataSource recurso	Leitura	datasource*		
StartDirectQuery	Concede permissão para iniciar uma consulta direta nos OpenSearch DataSource arns fornecidos	Gravar	datasource*		

Tipos de recursos definidos pela Amazon OpenSearch

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
application	`arn:${Partition}:opensearch:${Region}:${Account}:application/${AppId}`	
datasource	`arn:${Partition}:opensearch:${Region}:${Account}:datasource/${DataSourceName}`	

Chaves de condição para a Amazon OpenSearch

OpenSearch não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o Amazon OpenSearch Inestion

O Amazon OpenSearch Ingestion (prefixo do serviço:`osis`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon OpenSearch Ingestion
- Tipos de recursos definidos pela Amazon OpenSearch Ingestion
- Chaves de condição para Amazon OpenSearch Ingestion

Ações definidas pela Amazon OpenSearch Ingestion

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreatePipeline	Concede permissão para criar um pipeline OpenSearch de ingestão	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole iam:PassRole kms:DescribeKey kms:GenerateDataKeyWithoutPlaintext logs:CreateLogDelivery
DeletePipeline	Concede permissão para excluir um pipeline OpenSearch de ingestão	Gravar	pipeline*		logs:DeleteLogDelivery logs:GetLogDelivery logs:ListLogDeliveries

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetPipeline	Concede permissão para recuperar informações de configuração para um pipeline de OpenSearch ingestão	Leitura	pipeline*		
GetPipelineBlueprint	Concede permissão para obter o conteúdo de um blueprint de pipeline de OpenSearch ingestão	Leitura	pipeline-blueprint*		
GetPipelineChangeProgress	Concede permissão para obter informações granulares sobre o status de um pipeline de OpenSearch ingestão	Leitura	pipeline*		
Ingest	Concede permissão para ingerir dados por meio de um pipeline OpenSearch de ingestão	Gravar	pipeline*		
ListPipelineBlueprints	Concede permissão para listar os nomes dos blueprints disponíveis para uma configuração de OpenSearch pipeline de ingestão	Lista			
ListPipelines	Concede permissão para listar a configuração básica de cada pipeline de OpenSearch ingestão na conta atual e na região	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar todas as tags de recursos associadas a um OpenSearch pipeline de ingestão	Leitura	pipeline*		
StartPipeline	Concede permissão para iniciar um pipeline OpenSearch de ingestão	Gravar	pipeline*		
StopPipeline	Concede permissão para interromper um pipeline OpenSearch de ingestão	Gravar	pipeline*		
TagResource	Concede permissão para anexar tags de recursos a um OpenSearch pipeline de ingestão	Tags	pipeline*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover tags de recursos de um pipeline do OpenSearch Inestion Service	Tags	pipeline*		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdatePipeline	Concede permissão para modificar a configuração de um pipeline OpenSearch de ingestão	Gravar	pipeline*		iam:PassRole kms:DescribeKey kms:GenerateDataKeyWithoutPlaintext logs:GetLogDelivery logs:ListLogDeliveries logs:UpdateLogDelivery
ValidatePipeline	Concede permissão para validar a configuração de um pipeline de OpenSearch ingestão	Leitura			

Tipos de recursos definidos pela Amazon OpenSearch Ingestion

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso

também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
pipeline	`arn:${Partition}:osis:${Region}:${Account}:pipeline/${PipelineName}`	aws:ResourceTag/${TagKey}
pipeline-blueprint	`arn:${Partition}:osis:${Region}:${Account}:blueprint/${BlueprintName}`	

Chaves de condição para Amazon OpenSearch Ingestion

O Amazon OpenSearch Ingestion define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o Amazon OpenSearch Serverless

O Amazon OpenSearch Serverless (prefixo do serviço:`aoss`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon OpenSearch Serverless
- Tipos de recursos definidos pelo Amazon OpenSearch Serverless
- Chaves de condição para Amazon OpenSearch Serverless

Ações definidas pelo Amazon OpenSearch Serverless

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
APIAccessAll	Conceda permissão a todos os Opensearch suportados APIs	Gravar	Collection*		
				aoss:collection aoss:CollectionId	
BatchGetCollection	Concede permissão para obter atributos de uma ou mais coleções	Leitura		aoss:collection	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchGetEffectiveLifecyclePolicy	Concede permissão para obter as informações sobre uma política de ciclo de vida aplicada a um ou mais recursos do AOSS	Leitura			
BatchGetLifecyclePolicy	Concede permissão para obter informações sobre uma ou mais políticas de ciclo de vida	Leitura			
BatchGetVpcEndpoint	Concede permissão para obter atributos de um ou mais endpoints da VPC	Leitura			
CreateAccessPolicy	Concede permissão para criar uma política de acesso a dados	Gravar		aoss:collection aoss:index	
CreateCollection	Concede permissão para criar uma coleção com tecnologia sem servidor	Gravar		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateIndex	Concede permissão para criar um índice de pesquisa aberta	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateLifecyclePolicy	Concede permissão para criar uma política de ciclo de vida	Gravar		aoss:index	
CreateSecurityConfig	Concede permissão para criar uma configuração de segurança com tecnologia sem servidor	Gravar			
CreateSecurityPolicy	Concede permissão para criar uma política de rede ou criptografia	Gravar		aoss:collection	
CreateVpcEndpoint	Concede permissão para criar uma OpenSearch-Serverless-managed interface VPC endpoint	Gravar			
DashboardsAccessAll	Concede permissão para o Opensearch Serverless Dashboards	Gravar	Dashboards*		
				aoss:collection aoss:CollectionId	
DeleteAccessPolicy	Concede permissão para excluir uma política de acesso a dados	Gravar		aoss:collection aoss:index	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteCollection	Concede permissão para excluir uma coleção com tecnologia sem servidor	Gravar	Collection*		
DeleteIndex	Concede permissão para excluir um índice do opensearch	Gravar			
DeleteLifecyclePolicy	Concede permissão para excluir uma política de ciclo de vida	Gravar		aoss:index	
DeleteSecurityConfig	Concede permissão para excluir uma configuração de segurança	Gravar			
DeleteSecurityPolicy	Concede permissão para excluir uma política de segurança	Gravar		aoss:collection	
DeleteVpcEndpoint	Concede permissão para excluir um endpoint VPC de interface OpenSearch gerenciada sem servidor	Gravar			
GetAccessPolicy	Concede permissão para obter informações sobre uma política de acesso a dados	Leitura		aoss:collection aoss:index	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAccountSettings	Concede permissão para obter configurações de conta, incluindo configurações de capacidade	Leitura			
GetIndex	Concede permissão para obter um índice de pesquisa aberta	Leitura			
GetPoliciesStats	Concede permissão para obter estatísticas das políticas de segurança em sua conta	Leitura			
GetSecurityConfig	Concede permissão para obter informações sobre uma configuração de segurança com tecnologia sem servidor	Leitura			
GetSecurityPolicy	Concede permissão para obter informações sobre uma política de segurança	Leitura		aoss:collection	
ListAccessPolicies	Concede permissão para listar políticas de acesso a dados	Lista			
ListCollections	Concede permissão para listar coleções	Lista			
ListLifecyclePolicies	Concede permissão para listar políticas de ciclo de vida	Lista			
ListSecurityConfigs	Concede permissão para listar configurações de segurança	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListSecurityPolicies	Concede permissão para listar políticas de segurança	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de uma coleção	Lista			
ListVpcEndpoints	Concede permissão para listar endpoints VPC gerenciados sem OpenSearch servidor	Lista			
TagResource	Concede permissão para etiquetar uma coleção com tecnologia sem servidor	Gravar		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover etiquetas de uma coleção	Gravar		aws:TagKeys	
UpdateAccessPolicy	Concede permissão para atualizar uma política de acesso a dados	Gravar		aoss:collection aoss:index	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateAccountSettings	Concede permissão para atualizar configurações de conta, incluindo configurações de capacidade	Gravar			
UpdateCollection	Concede permissão para atualizar uma coleção	Gravar	Collection*		
UpdateIndex	Concede permissão para atualizar um índice do opensearch	Gravar			
UpdateLifecyclePolicy	Concede permissão para atualizar uma política de ciclo de vida	Gravar		aoss:index	
UpdateSecurityConfig	Concede permissão para atualizar uma configuração de segurança	Gravar			
UpdateSecurityPolicy	Concede permissão para atualizar uma política de segurança	Gravar		aoss:collection	
UpdateVpcEndpoint	Concede permissão para atualizar um VPC endpoint gerenciado sem OpenSearch servidor	Gravar			

Tipos de recursos definidos pelo Amazon OpenSearch Serverless

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações

identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
Collection	`arn:${Partition}:aoss:${Region}:${Account}:collection/${CollectionId}`	aws:ResourceTag/${TagKey}
Dashboards	`arn:${Partition}:aoss:${Region}:${Account}:dashboards/default`	

Chaves de condição para Amazon OpenSearch Serverless

O Amazon OpenSearch Serverless define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aoss:CollectionId	Filtra o acesso pelo identificador da coleção	String
aoss:collection	Filtra o acesso pelo nome da coleção	String
aoss:index	Filtra o acesso pelo índice	String
aws:RequestTag/${TagKey}	Filtra ações com base nas etiquetas transmitidas na solicitação	String

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra as ações com base nas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra ações com base nas chaves da etiqueta transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o Amazon OpenSearch Service

O Amazon OpenSearch Service (prefixo do serviço:`es`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon OpenSearch Service
- Tipos de recursos definidos pelo Amazon OpenSearch Service
- Chaves de condição para o Amazon OpenSearch Service

Ações definidas pelo Amazon OpenSearch Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptInboundConnection	Concede ao proprietário do domínio de destino permissão para aceitar uma solicitação de conexão de pesquisa entre clusters de entrada.	Gravar			
AcceptInboundCrossClusterSearchConnection	Concede ao proprietário do domínio de destino permissão para aceitar uma solicitação de conexão de pesquisa entre clusters de entrada. Essa permissão está defasada. Use em AcceptInboundConnection vez disso	Gravar			
AddDataSource	Concede permissão para adicionar a fonte de dados para o domínio do OpenSearch Serviço	Gravar	domain*		
AddDirectQueryDataSource	Concede permissão para adicionar a fonte de dados para os OpenSearch arns fornecidos	Gravar	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
AddTags	Concede permissão para anexar tags de recursos a um domínio de OpenSearc	Tags	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	h serviço, fonte de dados ou aplicativo		datasource*		
			domain*		
				aws:RequestTag/${TagKey} aws:TagKeys	
AssociatePackage	Concede permissão para associar um pacote a um domínio OpenSearch de serviço	Gravar	domain*		
AssociatePackages	Concede permissão para associar vários pacotes a um domínio OpenSearch de serviço	Gravar	domain*		
AuthorizeVpcEndpointAccess	Concede permissão para fornecer acesso a um domínio do Amazon OpenSearch Service por meio do uso de uma interface VPC endpoint	Gravar			
CancelDomainConfigChange	Concede permissão para cancelar uma alteração em um domínio OpenSearch do Serviço	Gravar	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelElasticsearchServiceSoftwareUpdate	Concede permissão para cancelar uma atualização do software de serviço de um domínio. Essa permissão está defasada. Use em CancelServiceSoftwareUpdate vez disso	Gravar	domain*		
CancelServiceSoftwareUpdate	Concede permissão para cancelar uma atualização do software de serviço de um domínio	Gravar	domain*		
CreateApplication	Concede permissão para criar um OpenSearch aplicativo	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDomain	Concede permissão para criar um domínio do Amazon OpenSearch Service	Gravar	domain		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateElasticsearchDomain	Concede permissão para criar um domínio OpenSearch de serviço. Essa permissão está defasada. Use em CreateDomain vez disso	Gravar	domain		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateElasticsearchServiceRole	Concede permissão para criar a função vinculada ao serviço necessária para domínios OpenSearch de serviço que usam acesso VPC. Essa permissão está obsoleta. OpenSearch O serviço cria a função vinculada ao serviço para você	Gravar			
CreateOutboundConnection	Concede permissão para criar entre um domínio de origem e um domínio de destino uma conexão de pesquisa entre clusters.	Gravar	domain*		
CreateOutboundCrossClusterSearchConnection	Concede permissão para criar uma nova conexão de pesquisa entre clusters, de um domínio de origem para domínio de destino. Essa permissão está defasada. Use em CreateOutboundConnection vez disso	Gravar	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreatePackage	Concede permissão para adicionar um pacote para uso com domínios OpenSearch de serviço	Gravar			
CreateServiceRole	Concede permissão para criar a função vinculada ao serviço necessária para domínios do Amazon OpenSearch Service que usam acesso VPC	Gravar			
CreateVpcEndpoint	Concede permissão para criar um OpenSearch VPC endpoint gerenciado pelo Amazon Service	Gravar			
DeleteApplication	Concede permissão para excluir um OpenSearch aplicativo	Gravar	application*		
DeleteDataSource	Concede permissão para excluir a fonte de dados do domínio do OpenSearch Serviço	Gravar	domain*		
DeleteDirectQueryDataSource	Concede permissão para excluir a fonte de dados dos OpenSearch arns fornecidos	Gravar	datasource*		
DeleteDomain	Concede permissão para excluir um domínio do Amazon OpenSearch Service e todos os seus dados	Gravar	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteElasticsearchDomain	Concede permissão para excluir um domínio do OpenSearch Serviço e todos os seus dados. Essa permissão está defasada. Use em DeleteDomain vez disso	Gravar	domain*		
DeleteElasticsearchServiceRole	Concede permissão para excluir a função vinculada ao serviço necessária para domínios OpenSearch de serviço que usam acesso VPC. Essa permissão está defasada. Use a API do IAM para excluir funções vinculadas a serviço	Gravar			
DeleteInboundConnection	Concede ao proprietário do domínio de destino permissão para excluir uma conexão de pesquisa entre clusters de entrada existente.	Gravar			
DeleteInboundCrossClusterSearchConnection	Concede ao proprietário do domínio de destino permissão para excluir uma conexão de pesquisa existente entre clusters de entrada. Essa permissão está defasada. Use em DeleteInboundConnection vez disso	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteOutboundConnection	Concede ao proprietário do domínio de origem permissão para excluir uma conexão de pesquisa entre clusters de saída existente.	Gravar			
DeleteOutboundCrossClusterSearchConnection	Concede ao proprietário do domínio de origem permissão para excluir uma conexão de pesquisa existente entre clusters de saída. Essa permissão está defasada. Use em DeleteOutboundConnection vez disso	Gravar			
DeletePackage	Concede permissão para excluir um pacote do OpenSearch Serviço. O pacote não pode ser associado a nenhum domínio	Gravar			
DeleteVpcEndpoint	Concede permissão para excluir um endpoint VPC de interface OpenSearch gerenciada pelo Amazon Service	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeDomain	Concede permissão para visualizar uma descrição da configuração do domínio do OpenSearch serviço especificado, incluindo o ID do domínio, o endpoint do serviço e o ARN	Leitura	domain*		
DescribeDomainAutoTunes	Concede permissão para visualizar a configuração do Auto-Tune do domínio para o domínio de OpenSearch Serviço especificado, incluindo o estado do Auto-Tune e os cronogramas de manutenção	Leitura	domain*		
DescribeDomainChangeProgress	Concede permissão para visualizar o progresso detalhado do estágio de um domínio OpenSearch de serviço	Leitura	domain*		
DescribeDomainConfig	Concede permissão para visualizar uma descrição das opções de configuração e do status de um domínio de OpenSearch serviço	Leitura	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeDomainHealth	Concede permissão para visualizar informações sobre a integridade do domínio e do nó, a zona de disponibilidade em espera, o número de nós por zona de disponibilidade e a contagem de fragmentos por nó	Leitura	domain*		
DescribeDomainNodes	Conceda permissão para visualizar informações sobre nós configurados para o domínio e suas configurações - o id do nó, tipo de nó, status do nó, zona de disponibilidade, tipo de instância e armazenamento	Leitura	domain*		
DescribeDomains	Concede permissão para visualizar uma descrição da configuração do domínio para até cinco domínios de OpenSearch serviço especificados	Lista	domain*		
DescribeDryRunProgress	Concede permissão para descrever o status de uma verificação de validação de pré-atualização em um domínio do OpenSearch Serviço	Leitura	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeElasticsearchDomain	Concede permissão para visualizar uma descrição da configuração do domínio do OpenSearch serviço especificado, incluindo o ID do domínio, o endpoint do serviço e o ARN. Essa permissão está defasada. Use em DescribeDomain vez disso	Leitura	domain*		
DescribeElasticsearchDomainConfig	Concede permissão para visualizar uma descrição da configuração e do status de um domínio de OpenSearch serviço. Essa permissão está defasada. Use em DescribeDomainConfig vez disso	Leitura	domain*		
DescribeElasticsearchDomains	Concede permissão para visualizar uma descrição da configuração do domínio para até cinco OpenSearch domínios específicos da Amazon. Essa permissão está defasada. Use em DescribeDomains vez disso	Lista	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeElasticsearchInstanceTypeLimits	Concede permissão para visualizar a contagem de instâncias, o armazenamento e os limites do nó principal para uma determinada OpenSearch versão e tipo de instância. Essa permissão está defasada. Use em DescribeInstanceTypeLimits vez disso	Lista			
DescribeInboundConnections	Concede permissão para listar todas as conexões de pesquisa entre clusters de entrada de um domínio de destino.	Lista			
DescribeInboundCrossClusterSearchConnections	Concede permissão para listar todas as conexões de pesquisa entre clusters de entrada para um domínio de destino. Essa permissão está defasada. Use em DescribeInboundConnections vez disso	Lista			
DescribeInstanceTypeLimits	Concede permissão para visualizar os limites de número de instâncias, armazenamento e nó principal de uma determinada versão de mecanismo e tipo de instância	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeOutboundConnections	Concede permissão para listar todas as conexões de pesquisa entre clusters de saída de um domínio de origem.	Lista			
DescribeOutboundCrossClusterSearchConnections	Concede permissão para listar todas as conexões de pesquisa entre clusters de saída para um domínio de origem. Essa permissão está defasada. Use em DescribeOutboundConnections vez disso	Lista			
DescribePackages	Concede permissão para descrever todos os pacotes disponíveis para domínios OpenSearch de serviço	Leitura			
DescribeReservedElasticsearchInstanceOfferings	Concede permissão para buscar ofertas de Instâncias Reservadas para o Amazon OpenSearch Service. Essa permissão está defasada. Use em DescribeReservedInstanceOfferings vez disso	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeReservedElasticsearchInstances	Concede permissão para buscar instâncias reservadas de OpenSearch serviço que já foram compradas. Essa permissão está defasada. Use em DescribeReservedInstances vez disso	Lista			
DescribeReservedInstanceOfferings	Concede permissão para buscar ofertas de Instâncias Reservadas para o Serviço OpenSearch	Lista			
DescribeReservedInstances	Concede permissão para buscar instâncias reservadas de OpenSearch serviço que já foram compradas	Lista			
DescribeVpcEndpoints	Concede permissão para descrever um ou mais endpoints OpenSearch VPC gerenciados pelo Amazon Service	Lista			
DissociatePackage	Concede permissão para desassociar um pacote do domínio de OpenSearch serviço especificado	Gravar	domain*		
DissociatePackages	Concede permissão para desassociar vários pacotes do domínio de OpenSearch serviço especificado	Gravar	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ESCrossClusterGet	Concede permissão para enviar solicitações entre clusters para um domínio de destino	Leitura	domain		
ESHttpDelete	Concede permissão para enviar solicitações HTTP DELETE para o OpenSearch APIs	Gravar	domain		
ESHttpGet	Concede permissão para enviar solicitações HTTP GET para o OpenSearch APIs	Leitura	domain		
ESHttpHead	Concede permissão para enviar solicitações HTTP HEAD para o OpenSearch APIs	Leitura	domain		
ESHttpPatch	Concede permissão para enviar solicitações HTTP PATCH para o OpenSearch APIs	Gravar	domain		
ESHttpPost	Concede permissão para enviar solicitações HTTP POST para o OpenSearch APIs	Gravar	domain		
ESHttpPut	Concede permissão para enviar solicitações HTTP PUT para o OpenSearch APIs	Gravar	domain		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetApplication	Concede permissão para obter informações sobre um OpenSearch aplicativo	Leitura	application*		
GetCompatibleElasticsearchVersions	Concede permissão para buscar uma lista de versões compatíveis OpenSearch e do Elasticsearch para as quais um domínio de OpenSearch serviço pode ser atualizado. Essa permissão está defasada. Use em GetCompatibleVersions vez disso	Lista	domain*		
GetCompatibleVersions	Concede permissão para buscar uma lista de versões de mecanismos compatíveis para as quais um domínio OpenSearch de serviço pode ser atualizado	Lista	domain*		
GetDataSource	Concede permissão para obter a fonte de dados para o domínio do OpenSearch Serviço	Leitura	domain*		
GetDirectQueryDataSource	Concede permissão para obter a fonte de dados para os OpenSearch arns fornecidos	Leitura	datasource*		
GetDomainMaintenanceStatus	Concede permissão para recuperar o status da ação de manutenção do nó	Leitura	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetPackageVersionHistory	Concede permissão para buscar o histórico de versões de um pacote.	Leitura			
GetUpgradeHistory	Concede permissão para buscar o histórico de atualização de um determinado domínio de OpenSearch serviço	Leitura	domain*		
GetUpgradeStatus	Concede permissão para obter o status de atualização de um determinado domínio de OpenSearch serviço	Leitura	domain*		
ListApplications	Concede permissão para listar OpenSearch aplicativos	Lista	application*		
ListDataSources	Concede permissão para recuperar uma lista de fontes de dados para o domínio do OpenSearch Serviço	Lista	domain*		
ListDirectQueryDataSources	Concede permissão para recuperar uma lista de fontes de dados para os arns fornecidos OpenSearch	Lista	datasource*		
ListDomainMaintenances	Concede permissão para recuperar uma lista de ações de manutenção para o domínio do OpenSearch Serviço	Lista	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDomainNames	Concede permissão para exibir os nomes de todos os domínios de OpenSearch serviço que o usuário atual possui	Lista			
ListDomainsForPackage	Concede permissão para listar todos os domínios de OpenSearch serviço aos quais um pacote está associado	Lista			
ListElasticsearchInstanceTypeDetails	Concede permissão para listar todos os tipos de instância e recursos disponíveis para uma determinada OpenSearch versão. Essa permissão está defasada. Use em ListInstanceTypeDetails vez disso	Lista			
ListElasticsearchInstanceTypes	Concede permissão para listar todos os tipos de EC2 instância compatíveis com uma determinada OpenSearch versão	Lista			
ListElasticsearchVersions	Concede permissão para listar todas OpenSearch as versões compatíveis no Amazon OpenSearch Service. Essa permissão está defasada. Use em ListVersions vez disso	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListInstanceTypeDetails	Concede permissão para listar todos os tipos de instância e recursos disponíveis para uma determinada versão OpenSearch ou versão do Elasticsearch	Lista			
ListPackagesForDomain	Concede permissão para listar todos os pacotes associados ao domínio do OpenSearch Serviço	Lista	domain*		
ListScheduledActions	Concede permissão para recuperar uma lista de alterações de configuração agendadas para um domínio OpenSearch de serviço	Lista	domain*		
ListTags	Concede permissão para exibir todas as tags de recursos de um domínio de OpenSearch serviço, fonte de dados ou aplicativo	Leitura	application*		
			datasource*		
			domain*		
ListVersions	Concede permissão para listar todas as versões suportadas OpenSearch e do Elasticsearch no Amazon Service OpenSearch	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListVpcEndpointAccess	Concede permissão para recuperar informações sobre cada AWS principal que tem permissão para acessar um determinado domínio do Amazon OpenSearch Service por meio do uso de uma interface VPC endpoint	Lista			
ListVpcEndpoints	Concede permissão para recuperar todos os endpoints VPC OpenSearch gerenciados pelo Amazon Service na região atual e na região Conta da AWS	Lista			
ListVpcEndpointsForDomain	Concede permissão para recuperar todos os endpoints VPC OpenSearch gerenciados pelo Amazon Service associados a um domínio específico	Lista			
PurchaseReservedElasticsearchInstanceOffering	Concede permissão para comprar Instâncias Reservadas de OpenSearch Serviço. Essa permissão está defasada. Use em PurchaseReservedInstanceOffering vez disso	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PurchaseReservedInstanceOffering	Concede permissão para comprar instâncias OpenSearch reservadas	Gravar			
RejectInboundConnection	Concede ao proprietário do domínio de destino permissão para rejeitar uma solicitação de conexão de pesquisa entre clusters de entrada.	Gravar			
RejectInboundCrossClusterSearchConnection	Concede ao proprietário do domínio de destino permissão para rejeitar uma solicitação de conexão de pesquisa entre clusters de entrada. Essa permissão está defasada. Use em RejectInboundConnection vez disso	Gravar			
RemoveTags	Concede permissão para remover tags de recursos de um domínio de OpenSearch serviço, fonte de dados ou aplicativo	Tags	application*		
			datasource*		
			domain*		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RevokeVpcEndpointAccess	Concede permissão para revogar o acesso a um domínio do Amazon OpenSearch Service fornecido por meio de uma interface VPC endpoint	Gravar			
StartDomainMaintenance	Concede permissão para iniciar a manutenção no nó	Gravar	domain*		
StartElasticsearchServiceSoftwareUpdate	Concede permissão para iniciar uma atualização do software de serviço de um domínio. Essa permissão está defasada. Use em StartServiceSoftwareUpdate vez disso	Gravar	domain*		
StartServiceSoftwareUpdate	Concede permissão para iniciar uma atualização do software de serviço de um domínio	Gravar	domain*		
UpdateApplication	Concede permissão para atualizar um OpenSearch aplicativo	Gravar	application*		
UpdateDataSource	Concede permissão para atualizar a fonte de dados para o domínio do OpenSearch Serviço	Gravar	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateDirectQueryDataSource	Concede permissão para atualizar a fonte de dados dos OpenSearch arns fornecidos	Gravar	datasource*		
UpdateDomainConfig	Concede permissão para modificar a configuração de um domínio de OpenSearch serviço, como o tipo de instância ou o número de instâncias	Gravar	domain*		
UpdateElasticsearchDomainConfig	Concede permissão para modificar a configuração de um domínio de OpenSearch serviço, como o tipo de instância ou o número de instâncias. Essa permissão está defasada. Use em UpdateDomainConfig vez disso	Gravar	domain*		
UpdatePackage	Concede permissão para atualizar um pacote para uso com domínios OpenSearch de serviço	Gravar			
UpdatePackageScope	Concede permissão para atualizar o escopo de um pacote	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateScheduledAction	Concede permissão para reagendar uma alteração planejada na configuração do domínio OpenSearch de serviço para um momento posterior	Gravar	domain*		
UpdateVpcEndpoint	Concede permissão para modificar um endpoint VPC de interface OpenSearch gerenciada pelo Amazon Service	Gravar			
UpgradeDomain	Concede permissão para iniciar a atualização de um domínio OpenSearch de serviço para uma determinada versão	Gravar	domain*		
UpgradeElasticsearchDomain	Concede permissão para iniciar a atualização de um domínio OpenSearch de serviço para uma versão especificada. Essa permissão está defasada. Use em UpgradeDomain vez disso	Gravar	domain*		

Tipos de recursos definidos pelo Amazon OpenSearch Service

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso

também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição para o Amazon OpenSearch Service

O Amazon OpenSearch Service define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base nas etiquetas transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra as ações com base nas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra ações com base nas chaves da etiqueta transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS OpsWorks

AWS OpsWorks (prefixo do serviço:`opsworks`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS OpsWorks
- Tipos de recursos definidos pelo AWS OpsWorks
- Chaves de condição do AWS OpsWorks

Ações definidas pelo AWS OpsWorks

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssignInstance	Concede permissão para atribuir uma instância registrada a uma camada	Gravar	stack		
AssignVolume	Concede permissão para atribuir um dos volumes do Amazon EBS registrados da pilha a uma instância especificada	Gravar	stack		
AssociateElasticIp	Concede permissão para associar um dos endereços de IP elástico registrados da pilha a uma instância especificada	Gravar	stack		
AttachElasticLoadBalancer	Concede permissão para anexar um balanceador de carga do Elastic Load Balancing a uma camada especificada	Gravar	stack		
CloneStack	Concede permissão para criar um clone de uma pilha especificada	Gravar	stack		
CreateApp	Concede permissão para criar uma aplicação para uma pilha especificada	Gravar	stack		
CreateDeployment	Concede permissão para executar comandos de implantação ou de pilha	Gravar	stack		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateInstance	Concede permissão para criar uma instância em uma pilha especificada	Gravar	stack		
CreateLayer	Concede permissão para criar uma camada	Gravar	stack		
CreateStack	Concede permissão para criar uma nova pilha	Gravar			
CreateUserProfile	Concede permissão para criar um novo perfil de usuário	Gravar			
DeleteApp	Concede permissão para excluir uma aplicação especificada	Gravar	stack		
DeleteInstance	Concede permissão para excluir uma instância específica, o que encerra a instância Amazon EC2 associada	Gravar	stack		
DeleteLayer	Concede permissão para excluir uma camada especificada	Gravar	stack		
DeleteStack	Concede permissão para excluir uma pilha especificada	Gravar	stack		
DeleteUserProfile	Concede permissão para excluir um perfil de usuário	Gravar			
DeregisterEcsCluster	Concede permissão para excluir um perfil de usuário	Gravar	stack		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeregisterElasticIp	Concede permissão para cancelar o registro de um endereço de IP elástico especificado	Gravar	stack		
DeregisterInstance	Concede permissão para cancelar o registro de uma instância registrada da Amazon EC2 ou local	Gravar	stack		
DeregisterRdsDbInstance	Concede permissão para cancelar o registro de uma instância do Amazon RDS	Gravar	stack		
DeregisterVolume	Concede permissão para cancelar um registro de um volume do Amazon EBS	Gravar	stack		
DescribeAgentVersions	Concede permissão para descrever as versões disponíveis do AWS OpsWorks agente	Lista	stack		
DescribeApps	Concede permissão para solicitar uma descrição de um conjunto de aplicações especificado	Lista	stack		
DescribeCommands	Concede permissão para descrever os resultados de comandos especificados	Lista	stack		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeDeployments	Concede permissão para solicitar uma descrição de um conjunto de implantações especificado	Lista	stack		
DescribeEcsClusters	Concede permissão para descrever os clusters do Amazon ECS que estão registrados em uma pilha	Lista	stack		
DescribeElasticIps	Concede permissão para descrever endereços de IP elástico	Lista	stack		
DescribeElasticLoadBalancers	Concede permissão para descrever instâncias do Elastic Load Balancing de uma pilha	Lista	stack		
DescribeInstances	Concede permissão para solicitar uma descrição de um conjunto de instâncias	Lista	stack		
DescribeLayers	Concede permissão para solicitar uma descrição de uma ou mais camadas em uma pilha especificada	Lista	stack		
DescribeLoadBasedAutoScaling	Concede permissão para descrever as configurações de autoescalabilidade com base em carga de camadas especificadas	Lista	stack		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeMyUserProfile	Concede permissão para descrever as informações de SSH de um usuário	Lista			
DescribeOperatingSystems	Concede permissão para descrever os sistemas operacionais compatíveis com o AWS OpsWorks Stacks	Lista			
DescribePermissions	Concede permissão para descrever as permissões para uma pilha especificada	Lista	stack		
DescribeRaidArrays	Concede permissão para descrever as matrizes de RAID de uma instância	Lista	stack		
DescribeRdsDbInstances	Concede permissão para descrever instâncias do Amazon RDS	Lista	stack		
DescribeServiceErrors	Concede permissão para descrever erros AWS OpsWorks de serviço	Lista	stack		
DescribeStackProvisioningParameters	Concede permissão para solicitar uma descrição dos parâmetros de provisionamento de uma pilha	Lista	stack		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeStackSummary	Concede permissão para descrever o número de camadas e de aplicações em uma pilha especificada e o número de instâncias em cada estado, como running_setup ou online	Lista	stack		
DescribeStacks	Concede permissão para solicitar uma descrição de uma ou mais pilhas	Lista	stack		
DescribeTimeBasedAutoScaling	Concede permissão para descrever as configurações de autoescalabilidade com base em tempo das instâncias especificadas	Lista	stack		
DescribeUserProfiles	Concede permissão para descrever usuários especificados	Lista			
DescribeVolumes	Concede permissão para descrever os volumes do Amazon EBS de uma instância	Lista	stack		
DetachElasticLoadBalancer	Concede permissão para desanexar uma instância do Elastic Load Balancing especificada da camada	Gravar	stack		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateElasticIp	Concede permissão para desassociar um endereço de IP elástico da instância	Gravar	stack		
GetHostnameSuggestion	Concede permissão para obter um nome de host gerado para a camada especificada, com base no tema do nome de host atual	Leitura	stack		
GrantAccess	Concede permissão para conceder acesso RDP a uma instância do Windows por um período especificado	Gravar	stack		
ListTags	Concede permissão para retornar uma lista de etiquetas que são aplicadas à pilha ou à camada especificada	Lista	stack		
RebootInstance	Concede permissão para reiniciar uma instância especificada	Gravar	stack		
RegisterEcsCluster	Concede permissão para registrar um cluster do Amazon ECS especificado em uma pilha	Gravar	stack		
RegisterElasticIp	Concede permissão para registrar um endereço de IP elástico em uma pilha especificada	Gravar	stack		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RegisterInstance	Concede permissão para registrar instâncias com uma pilha especificada que foram criadas fora do AWS OpsWorks	Gravar	stack		
RegisterRdsDbInstance	Concede permissão para registrar uma instância do Amazon RDS em uma pilha	Gravar	stack		
RegisterVolume	Concede permissão para registrar um volume do Amazon EBS em uma pilha especificada	Gravar	stack		
SetLoadBasedAutoScaling	Concede permissão para especificar a configuração de autoescalabilidade com base em carga de uma camada especificada	Gravar	stack		
SetPermission	Concede permissão para especificar as permissões de um usuário	Gerenciamento de permissões	stack		
SetTimeBasedAutoScaling	Concede permissão para especificar a configuração de autoescalabilidade com base em tempo de uma instância especificada	Gravar	stack		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartInstance	Concede permissão para iniciar uma instância especificada	Gravar	stack		
StartStack	Concede permissão para iniciar instâncias de uma pilha	Gravar	stack		
StopInstance	Concede permissão para interromper uma instância especificada	Gravar	stack		
StopStack	Concede permissão para interromper uma pilha especificada	Gravar	stack		
TagResource	Concede permissão para aplicar etiquetas a uma pilha ou camada especificada	Tags	stack		
UnassignInstance	Concede permissão para cancelar a atribuição de uma instância registrada de todas as camadas	Gravar	stack		
UnassignVolume	Concede permissão para cancelar a atribuição de um volume do Amazon EBS atribuído	Gravar	stack		
UntagResource	Concede permissão para remover etiquetas de uma pilha ou camada especificada	Tags	stack		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateApp	Concede permissão para atualizar uma aplicação especificada	Gravar	stack		
UpdateElasticIp	Concede permissão para atualizar o nome de um endereço de IP elástico registrado	Gravar	stack		
UpdateInstance	Concede permissão para atualizar uma instância especificada	Gravar	stack		
UpdateLayer	Concede permissão para atualizar uma camada especificada	Gravar	stack		
UpdateMyUserProfile	Concede permissão para atualizar uma chave pública SSH do usuário	Gravar			
UpdateRdsDbInstance	Concede permissão para atualizar uma instância do Amazon RDS	Gravar	stack		
UpdateStack	Concede permissão para atualizar uma pilha especificada	Gravar	stack		
UpdateUserProfile	Concede permissão para atualizar um perfil de usuário especificado	Gerenciamento de permissões			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateVolume	Concede permissão para atualizar o nome ou o ponto de montagem de um volume do Amazon EBS	Gravar	stack		

Tipos de recursos definidos pelo AWS OpsWorks

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
stack	`arn:${Partition}:opsworks:${Region}:${Account}:stack/${StackId}/`	

Chaves de condição do AWS OpsWorks

OpsWorks não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o gerenciamento de AWS OpsWorks configuração

AWS OpsWorks O Configuration Management (prefixo do serviço:`opsworks-cm`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS OpsWorks Configuration Management
- Tipos de recursos definidos pelo AWS OpsWorks Configuration Management
- Chaves de condição para gerenciamento de AWS OpsWorks configuração

Ações definidas pelo AWS OpsWorks Configuration Management

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar

a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateNode	Concede permissão para associar um nó a um servidor de gerenciamento de configuração.	Write			
CreateBackup	Concede permissão para criar um backup do servidor especificado.	Write			
CreateServer	Concede permissão para criar um servidor.	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteBackup	Concede permissão para excluir o backup especificado e possivelmente o bucket do S3.	Gravar			
DeleteServer	Concede permissão para excluir o servidor especificado com sua CloudFormation pilha correspondente e, possivelmente, o bucket S3	Gravar			
DescribeAccountAttributes	Concede permissão para descrever os limites de serviço da conta do usuário.	List			
DescribeBackups	Concede permissão para descrever um backup único, todos os backups de um servidor especificado ou todos os backups da conta do usuário.	List			
DescribeEvents	Concede permissão para descrever todos os eventos do servidor especificado.	List			
DescribeNodeAssociationStatus	Concede permissão para descrever o status da associação do token do nó especificado e do servidor especificado.	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeServers	Concede permissão para descrever o servidor especificado ou todos os servidores da conta do usuário.	List			
DisassociateNode	Concede permissão para desassociar um nó especificado de um servidor.	Write			
ExportServerEngineAttribute	Concede permissão para exportar o atributo de um mecanismo de um servidor.	Read			
ListTagsForResource	Concede permissão para listar as etiquetas aplicadas ao servidor ou backup especificado.	Read			
RestoreServer	Concede permissão para aplicar um backup ao servidor especificado. Possivelmente muda a instância do EC2 se especificado.	Write			
StartMaintenance	Concede permissão para iniciar a manutenção do servidor imediatamente.	Write			
TagResource	Concede permissão para aplicar etiquetas ao servidor ou backup especificado.	Marcação			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para remover as etiquetas do servidor ou backup especificado.	Marcação			
UpdateServer	Concede permissão para atualizar as configurações gerais do servidor.	Write			
UpdateServerEngineAttributes	Concede permissão para atualizar as configurações do servidor específicas ao tipo de gerenciamento de configuração.	Gravar			

Tipos de recursos definidos pelo AWS OpsWorks Configuration Management

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
server	`arn:${Partition}:opsworks-cm::${Account}:server/${ServerName}/${UniqueId}`	

Tipos de recursos	ARN	Chaves de condição
backup	`arn:${Partition}:opsworks-cm::${Account}:backup/${ServerName}-{Date-and-Time-Stamp-of-Backup}`	

Chaves de condição para gerenciamento de AWS OpsWorks configuração

O OpsworksCM não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Organizations

AWS Organizations (prefixo do serviço:`organizations`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Organizations
- Tipos de recursos definidos pelo AWS Organizations
- Chaves de condição do AWS Organizations

Ações definidas pelo AWS Organizations

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptHandshake	Concede permissão para enviar uma resposta ao originador de um handshake concordando com a ação proposta pela solicitação de handshake	Gravar	handshake*		iam:CreateServiceLinkedRole
AttachPolicy	Concede permissão para anexar uma política a uma raiz, a uma unidade organizacional ou a uma conta individual	Gravar	policy*		
			account		
			organizationalunit		
			root		
				organizations:PolicyType	
CancelHandshake	Concede permissão para cancelar um handshake	Gravar	handshake*		
CloseAccount	Concede permissão para fechar uma Conta da AWS que agora faz parte de uma Organizations, criada dentro da organização ou convidada a participar da organização	Gravar	account*		
CreateAccount	Concede permissão para criar um Conta da AWS que seja automaticamente membro da	Gravar		aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	organização com as credencias que fizeram a solicitação			aws:TagKeys aws:ResourceTag/${TagKey}	
CreateGovCloudAccount	Concede permissão para criar uma conta AWS GovCloud (EUA)	Gravar		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateOrganization	Concede permissão para criar uma organização. A conta com as credenciais que chama a CreateOrganization operação se torna automaticamente a conta de gerenciamento da nova organização	Gravar			iam:CreateServiceLinkedRole
CreateOrganizationalUnit	Concede permissão para criar uma unidade organizacional (UO) em uma UO raiz ou pai	Gravar	organizationalunit root		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePolicy	Concede permissão para criar uma política que você pode anexar a uma raiz, a uma unidade organizacional (OU) ou a um indivíduo Conta da AWS	Gravar		organizations:PolicyType aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeclineHandshake	Concede permissão para recusar uma solicitação de handshake. Isso define o estado do handshake como DECLINED (RECUSADO) e desativa efetivamente a solicitação	Gravar	handshake*		
DeleteOrganization	Concede permissão para excluir a organização	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteOrganizationalUnit	Concede permissão para excluir uma unidade organizacional de uma raiz ou de outra UO	Gravar	organizationalunit*		
DeletePolicy	Concede permissão para excluir uma política de sua organização	Gravar	policy*		
				organizations:PolicyType	
DeleteResourcePolicy	Concede permissão para excluir uma política de recursos de sua organização	Gravar			
DeregisterDelegatedAdministrator	Concede permissão para cancelar o registro do membro especificado Conta da AWS como administrador delegado para o AWS serviço especificado por ServicePrincipal	Gravar	account*		
				organizations:ServicePrincipal	
DescribeAccount	Concede permissão para recuperar os detalhes relacionados a organizações sobre a conta especificada	Leitura	account*		
DescribeCreateAccountStatus	Concede permissão para recuperar o status atual de uma solicitação assíncrona para criar uma conta	Leitura			
DescribeEffectivePolicy		Leitura	account*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	Concede permissão para recuperar a política efetiva de uma conta			organizations:PolicyType	
DescribeHandshake	Concede permissão para recuperar detalhes sobre um handshake solicitado anteriormente	Leitura	handshake*		
DescribeOrganization	Concede permissão para recuperar detalhes sobre a organização à qual as credenciais de chamada pertencem	Leitura			
DescribeOrganizationalUnit	Concede permissão para recuperar detalhes sobre uma unidade organizacional (UO)	Leitura	organizationalunit*		
DescribePolicy	Concede permissão para recuperar detalhes sobre uma política	Leitura	policy*		
				organizations:PolicyType	
DescribeResourcePolicy	Concede permissão para recuperar informações sobre uma política de recursos	Leitura			
DetachPolicy	Concede permissão para desvincular uma política de uma raiz, de uma unidade organizacional ou de uma conta de destino	Gravar	policy*		
			account		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			organizationalunit		
			root		
				organizations:PolicyType	
DisableAWSServiceAccess	Concede permissão para desativar a integração de um AWS serviço (o serviço especificado por ServicePrincipal) com AWS Organizations	Gravar		organizations:ServicePrincipal	
DisablePolicyType	Concede permissão para desabilitar um tipo de política da organização em uma raiz	Gravar	root*		
				organizations:PolicyType	
EnableAWSServiceAccess	Concede permissão para permitir a integração de um AWS serviço (o serviço especificado por ServicePrincipal) com AWS Organizations	Gravar		organizations:ServicePrincipal	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
EnableAllFeatures	Concede permissão para iniciar o processo de habilitação de todos os recursos de uma organização, atualizando-a de apenas compatibilidade com recursos de faturamento consolidado	Gravar			
EnablePolicyType	Concede permissão para habilitar um tipo de política em uma raiz	Gravar	root*		
				organizations:PolicyType	
InviteAccountToOrganization	Concede permissão para enviar um convite para outra pessoa Conta da AWS, solicitando que ela se junte à sua organização como uma conta membro	Gravar	account		
				aws:RequestTag/${TagKey} aws:TagKeys	
LeaveOrganization	Concede permissão para remover uma conta-membro de sua organização-pai	Gravar			
ListAWSServiceAccessForOrganization	Concede permissão para recuperar a lista dos AWS serviços para os quais você habilitou a integração com sua organização	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAccounts	Concede permissão para listar todas as contas na organização	Lista			
ListAccountsForParent	Concede permissão para listar as contas de uma organização que são contidas por uma raiz ou unidade organizacional (UO)	Lista	organizationalunit		
			root		
ListChildren	Concede permissão para listar todas as contas OUs ou que estão contidas em uma OU principal ou raiz	Lista	organizationalunit		
			root		
ListCreateAccountStatus	Concede permissão para listar as solicitações de criação de contas assíncronas que estão sendo controladas para a organização	Lista			
ListDelegatedAdministrators	Concede permissão para listar as AWS contas designadas como administradores delegados nesta organização	Lista		organizations:ServicePrincipal	
ListDelegatedServicesForAccount	Concede permissão para listar os AWS serviços para os quais a conta especificada é um administrador delegado nesta organização	Lista	account*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListHandshakesForAccount	Concede permissão para listar todos os handshakes que estão associados a uma conta	Lista			
ListHandshakesForOrganization	Concede permissão para listar os handshakes que estão associados à organização	Lista			
ListOrganizationalUnitsForParent	Concede permissão para listar todas as unidades organizacionais (OUs) em uma unidade organizacional principal ou raiz	Lista	organizationalunit		
			root		
ListParents	Concede permissão para listar as unidades raiz ou organizacionais (OUs) que servem como pais imediatos de uma OU ou conta secundária	Lista	account		
			organizationalunit		
ListPolicies	Concede permissão para listar todas as políticas de uma organização	Lista		organizations:PolicyType	
ListPoliciesForTarget	Concede permissão para listar todas as políticas que estão anexadas diretamente a uma raiz, unidade organizacional (UO) ou uma conta	Lista	account		
			organizationalunit		
			root		
				organizations:PolicyType	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListRoots	Concede permissão para listar todas as raízes definidas da organização	Lista			
ListTagsForResource	Concede permissão para listar todas as etiquetas do recurso especificado	Lista	account		
			organizationalunit		
			policy		
			resourcepolicy		
			root		
ListTargetsForPolicy	Concede permissão para listar todas as OUs raízes e contas às quais uma política está anexada	Lista	policy*		
				organizations:PolicyType	
MoveAccount	Concede permissão para mover uma conta de sua atual raiz ou UO para outra raiz pai ou UO	Gravar	account*		
			organizationalunit*		
			root*		
PutResourcePolicy	Concede permissão para criar ou atualizar uma política de recurso	Gravar	resourcepolicy*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
RegisterDelegatedAdministrator	Concede permissão para registrar a conta de membro especificada para administrar os recursos do AWS serviço da Organizations que é especificado por ServicePrincipal	Gravar	account*		
				organizations:ServicePrincipal	
RemoveAccountFromOrganization	Concede permissão para remover a conta especificada da organização	Gravar	account*		
TagResource	Concede permissão para adicionar uma ou mais etiquetas ao recurso especificado	Marcação	account		
			organizationalunit		
			policy	organizations:PolicyType	
			resourcepolicy		
			root		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover uma ou mais etiquetas do recurso especificado	Tags	account		
			organizationalunit		
			policy		
			resourcepolicy		
			root		
				aws:TagKeys	
UpdateOrganizationalUnit	Concede permissão para renomear uma unidade organizacional (UO)	Gravar	organizationalunit*		
UpdatePolicy	Concede permissão para atualizar uma política existente com um novo nome, descrição ou conteúdo	Gravar	policy*		
				organizations:PolicyType	

Tipos de recursos definidos pelo AWS Organizations

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
account	`arn:${Partition}:organizations::${Account}:account/o-${OrganizationId}/${AccountId}`	aws:ResourceTag/${TagKey}
handshake	`arn:${Partition}:organizations::${Account}:handshake/o-${OrganizationId}/${HandshakeType}/h-${HandshakeId}`	
organization	`arn:${Partition}:organizations::${Account}:organization/o-${OrganizationId}`	
organizationalunit	`arn:${Partition}:organizations::${Account}:ou/o-${OrganizationId}/ou-${OrganizationalUnitId}`	aws:ResourceTag/${TagKey}
policy	`arn:${Partition}:organizations::${Account}:policy/o-${OrganizationId}/${PolicyType}/p-${PolicyId}`	aws:ResourceTag/${TagKey}
resourcepolicy	`arn:${Partition}:organizations::${Account}:resourcepolicy/o-${OrganizationId}/rp-${ResourcePolicyId}`	aws:ResourceTag/${TagKey}
awspolicy	`arn:${Partition}:organizations::aws:policy/${PolicyType}/p-${PolicyId}`	

Tipos de recursos	ARN	Chaves de condição
root	`arn:${Partition}:organizations::${Account}:root/o-${OrganizationId}/r-${RootId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Organizations

AWS Organizations define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString
organizations:PolicyType	Filtra o acesso pelos nomes de tipo de política especificado	String
organizations:ServicePrincipal	Filtra o acesso pelos nomes de entidade principal de serviço especificada	String

Ações, recursos e chaves de condição do AWS Outposts

AWS Outposts (prefixo do serviço:`outposts`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Outposts
- Tipos de recursos definidos pelo AWS Outposts
- Chaves de condição do AWS Outposts

Ações definidas pelo AWS Outposts

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelCapacityTask	Concede permissão para cancelar uma tarefa de capacidade	Gravar	outpost*		
CancelOrder	Concede permissão para cancelar um pedido	Gravar			
CreateOrder	Concede permissão para criar um pedido	Gravar	outpost*		
CreateOutpost	Concede permissão para criar um Outpost	Gravar	site*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreatePrivateConnectivityConfig	Concede permissão para criar uma configuração de conectividade privada	Gravar	outpost*		
CreateSite	Concede permissão para criar um site	Gravar		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteOutpost	Concede permissão para excluir um Outpost	Gravar	outpost*		
DeleteSite	Concede permissão para excluir um site	Gravar	site*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetCapacityTask	Concede permissão para obter informações sobre a tarefa de capacidade especificada	Leitura	outpost*		
GetCatalogItem	Concede permissão para obter um item de catálogo	Leitura			
GetConnection	Concede permissão para obter informações sobre a conexão para o seu servidor Outpost	Leitura			
GetOrder	Concede permissão para obter informações sobre um pedido	Leitura			
GetOutpost	Concede permissão para obter informações sobre o Outpost especificado	Leitura	outpost*		
GetOutpostBillingInformation	Concede permissão para obter informações de cobrança do Outpost para o Outpost especificado	Leitura	outpost*		
GetOutpostInstanceTypes	Concede permissão para obter os tipos de instância do Outpost especificado	Leitura	outpost*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetOutpostSupportedInstanceTypes	Concede permissão para obter os tipos de instância compatíveis do Outpost especificado	Leitura	outpost*		
GetPrivateConnectivityConfig	Concede permissão para obter uma configuração de conectividade privada	Leitura	outpost*		
GetSite	Concede permissão para obter um site	Leitura	site*		
GetSiteAddress	Concede permissão para obter o endereço de um local	Leitura	site*		
ListAssetInstances	Concede permissão para listar todas as instâncias em execução para o Outpost especificado	Lista	outpost*		
ListAssets	Concede permissão para listar os ativos para os Outposts	Lista	outpost*		
ListBlockingInstancesForCapacityTask	Concede permissão para listar todas as instâncias em execução que estão impedindo a execução da tarefa de capacidade no Outpost especificado	Lista	outpost*		
ListCapacityTasks	Concede permissão para listar as tarefas de capacidade para seu Conta da AWS	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListCatalogItems	Concede permissão para listar todos os itens de catálogo	Lista			
ListOrders	Concede permissão para listar os pedidos do seu Conta da AWS	Lista			
ListOutposts	Concede permissão para listar os Outposts para o seu Conta da AWS	Lista			
ListSites	Concede permissão para listar os sites para o seu Conta da AWS	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura			
StartCapacityTask	Concede permissão para criar uma tarefa de capacidade	Gravar	outpost*		
StartConnection	Concede permissão para iniciar uma conexão para o seu servidor Outpost	Gravar			
TagResource	Concede permissão para marcar um recurso	Marcação	outpost		
			site		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso	Tags	outpost		
			site		
				aws:TagKeys	
UpdateOutpost	Concede permissão para atualizar um Outpost	Gravar	outpost*		
UpdateSite	Concede permissão para atualizar um site	Gravar	site*		
UpdateSiteAddress	Concede permissão para atualizar o endereço do local	Gravar	site*		
UpdateSiteRackPhysicalProperties	Concede permissão para atualizar as propriedades físicas de um rack em um local	Gravar	site*		

Tipos de recursos definidos pelo AWS Outposts

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves

são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
outpost	`arn:${Partition}:outposts:${Region}:${Account}:outpost/${OutpostId}`	aws:ResourceTag/${TagKey}
site	`arn:${Partition}:outposts:${Region}:${Account}:site/${SiteId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Outposts

AWS Outposts define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Panorama

AWS Panorama (prefixo do serviço:`panorama`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Panorama
- Tipos de recursos definidos pelo AWS Panorama
- Chaves de condição para o AWS Panorama

Ações definidas pelo AWS Panorama

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateApplicationInstance	Concede permissão para criar uma Instância do Aplicativo AWS Panorama	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
CreateJobForDevices	Concede permissão para criar um trabalho para um AWS Panorama Appliance	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateNodeFromTemplateJob	Concede permissão para criar um Nó AWS Panorâmico	Gravar			
CreatePackage	Concede permissão para criar um AWS Panorama Package	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
CreatePackageImportJob	Concede permissão para criar um AWS Panorama Package	Gravar			
DeleteDevice	Concede permissão para cancelar o registro de um Panorama Appliance AWS	Gravar	device*		
DeletePackage	Concede permissão para excluir um AWS Panorama Package	Gravar	package*		
DeregisterPackageVersion	Concede permissão para cancelar o registro de uma versão do pacote AWS Panorama	Gravar	package*		
DescribeApplicationInstance	Concede permissão para visualizar detalhes sobre uma instância do aplicativo AWS Panorama	Leitura	applicationInstance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeApplicationInstanceDetails	Concede permissão para visualizar detalhes sobre uma instância do aplicativo AWS Panorama	Leitura	applicationInstance*		
DescribeDevice	Concede permissão para visualizar detalhes sobre um AWS Panorama Appliance	Leitura	device*		
DescribeDeviceJob	Concede permissão para visualizar os detalhes do trabalho de um AWS Panorama Appliance	Leitura			
DescribeNode	Concede permissão para visualizar detalhes sobre um nó do aplicativo AWS Panorama	Leitura			
DescribeNodeFromTemplateJob	Concede permissão para visualizar detalhes sobre o nó do aplicativo AWS Panorama	Leitura			
DescribePackage	Concede permissão para visualizar detalhes sobre um pacote AWS Panorama	Leitura	package*		
DescribePackageImportJob	Concede permissão para visualizar detalhes sobre um pacote AWS Panorama	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribePackageVersion	Concede permissão para visualizar detalhes sobre uma versão do pacote AWS Panorama	Leitura	package*		
DescribeSoftware [somente permissão]	Concede permissão para visualizar detalhes sobre uma versão de software para o AWS Panorama Appliance	Leitura			
GetWebSocketURL [somente permissão]	Concede permissão para gerar um WebSocket endpoint para comunicação com AWS o Panorama	Leitura			
ListApplicationInstanceDependencies	Concede permissão para recuperar uma lista de dependências da instância do aplicativo no Panorama AWS	Lista	applicationInstance*		
ListApplicationInstanceNodeInstances	Concede permissão para recuperar uma lista de instâncias de nós de instâncias de aplicativos no Panorama AWS	Lista	applicationInstance*		
ListApplicationInstances	Concede permissão para recuperar uma lista de instâncias do aplicativo no Panorama AWS	Lista	device		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDevices	Concede permissão para recuperar uma lista de aparelhos no AWS Panorama	Lista			
ListDevicesJobs	Concede permissão para recuperar uma lista de trabalhos para um AWS Panorama Appliance	Lista	device		
ListNodeFromTemplateJobs	Concede permissão para recuperar uma lista de nós para um dispositivo AWS Panorama	Lista			
ListNodes	Concede permissão para recuperar uma lista de nós no AWS Panorama	Lista			
ListPackageImportJobs	Concede permissão para recuperar uma lista de pacotes no AWS Panorama	Lista			
ListPackages	Concede permissão para recuperar uma lista de pacotes no AWS Panorama	Lista			
ListTagsForResource	Concede permissão para recuperar uma lista de tags para um recurso no AWS Panorama	Leitura	applicationInstance		
			device		
			package		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ProvisionDevice	Concede permissão para registrar um AWS Panorama Appliance	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
RegisterPackageVersion	Concede permissão para registrar uma versão do pacote AWS Panorama	Gravar	package*		
RemoveApplicationInstance	Concede permissão para remover uma instância do aplicativo AWS Panorama	Gravar	applicationInstance*		
SignalApplicationInstanceNodeInstances	Concede permissão para sinalizar nós de câmera em uma instância da aplicação para pausar ou retomar	Gravar	applicationInstance*		
TagResource	Concede permissão para adicionar tags a um recurso no AWS Panorama	Tags	applicationInstance		
			device		
			package		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para remover tags de um recurso no AWS Panorama	Tags	applicationInstance		
			device		
			package		
				aws:TagKeys	
UpdateDeviceMetadata	Concede permissão para modificar as configurações básicas de um AWS Panorama Appliance	Gravar	device*		

Tipos de recursos definidos pelo AWS Panorama

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
device	`arn:${Partition}:panorama:${Region}:${Account}:device/${DeviceId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
package	`arn:${Partition}:panorama:${Region}:${Account}:package/${PackageId}`	aws:ResourceTag/${TagKey}
applicationInstance	`arn:${Partition}:panorama:${Region}:${Account}:applicationInstance/${ApplicationInstanceId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o AWS Panorama

AWS Panorama define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Parallel Computing Service

AWS O Parallel Computing Service (prefixo do serviço:`pcs`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Parallel Computing Service
- Tipos de recursos definidos pelo AWS Parallel Computing Service
- Chaves de condição do AWS Parallel Computing Service

Ações definidas pelo AWS Parallel Computing Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AllowVendedLogDeliveryForResource [somente permissão]	Concede permissão para configurar a entrega de registros vendidos para registros de cluster AWS PCS	Gravar	cluster*		
CreateCluster	Concede permissão para criar clusters	Gravar		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:GetSecurityGroupsForVpc iam:CreateServiceLinkedRole secretsmanager:CreateSecret secretsmanager:TagResource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateComputeNodeGroup	Concede permissão para criar grupos de nós de computação	Gravar	cluster*		ec2:CreateFleet ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateTags ec2:DescribeImages ec2:DescribeInstanceStatus ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:RunInstances iam:GetInstanceProfile iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateQueue	Concede permissão para criar filas	Gravar	cluster*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCluster	Concede permissão para excluir clusters	Gravar	cluster*		ec2:DeleteNetworkInterface secretsmanager:DeleteSecret

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteComputeNodeGroup	Concede permissão para excluir grupos de nós de computação	Gravar	cluster*		ec2:DeleteLaunchTemplate ec2:TerminateInstances
			computenodegroup*		
DeleteQueue	Concede permissão para excluir filas	Gravar	cluster*		
			queue*		
GetCluster	Concede permissão para obter propriedades de clusters	Leitura	cluster*		
GetComputeNodeGroup	Concede permissão para obter propriedades de grupo de nós de computação	Leitura	cluster*		
			computenodegroup*		
GetQueue	Concede permissão para obter propriedades de filas	Leitura	cluster*		
			queue*		
ListClusters	Concede permissão para listar clusters	Lista			
ListComputeNodeGroups	Concede permissão para listar grupos de nós de computação	Lista	cluster*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListQueues	Concede permissão para listar filas	Lista	cluster*		
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura			
RegisterComputeNodeGroupInstance	Concede permissão para registrar uma instância de computação em um grupo de nós de computação	Gravar	cluster*		secretsmanager:GetSecretValue
TagResource	Concede permissão para marcar um recurso	Marcação	cluster	aws:ResourceTag/${TagKey}	
			computenodegroup	aws:ResourceTag/${TagKey}	
			queue	aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso	Tags	cluster	aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			computenodegroup	aws:ResourceTag/${TagKey}	
			queue	aws:ResourceTag/${TagKey}	
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateComputeNodeGroup	Concede permissão para atualizar propriedades de grupo de nós de computação	Gravar	cluster*		ec2:CreateFleet ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateTags ec2:DescribeImages ec2:DescribeInstanceStatus ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:RunInstances iam:GetInstanceProfile iam:PassRole
			computenodegroup*		
UpdateQueue	Concede permissão para atualizar propriedades de fila	Gravar	cluster*		
			queue*		

Tipos de recursos definidos pelo AWS Parallel Computing Service

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS Parallel Computing Service

AWS O Parallel Computing Service define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o gerenciamento de contas da Central de Parceiros da AWS

AWS O gerenciamento central de contas do parceiro (prefixo do serviço:`partnercentral-account-management`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo gerenciamento de contas da Central de Parceiros da AWS
- Tipos de recursos definidos pelo gerenciamento de contas da Central de Parceiros da AWS
- Chaves de condição para o gerenciamento de contas da Central de Parceiros da AWS

Ações definidas pelo gerenciamento de contas da Central de Parceiros da AWS

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando

usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociatePartnerAccount [somente permissão]	Concede permissão para associar a conta do Parceiro a Conta da AWS	Gravar			
AssociatePartnerUser	Concede permissão para associar um usuário parceiro ao perfil do IAM	Gravar			
DisassociatePartnerUser	Concede permissão para desassociar um usuário parceiro ao perfil do IAM	Gravar			

Tipos de recursos definidos pelo gerenciamento de contas da Central de Parceiros da AWS

AWS O gerenciamento de contas do Partner Central não suporta a especificação de um ARN de recurso `Resource` no elemento de uma declaração de política do IAM. Para conceder acesso ao gerenciamento de contas da Central de Parceiros da AWS , especifique `"Resource": "*"` em sua política.

Chaves de condição para o gerenciamento de contas da Central de Parceiros da AWS

O gerenciamento de contas da Central de Parceiros não têm chaves de contexto específicas do serviço que possam ser usadas no elemento `Condition` das instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o AWS Partner Central Selling

AWS O Partner Central Selling (prefixo do serviço:`partnercentral`) fornece os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Partner Central Selling
- Tipos de recursos definidos pelo AWS Partner Central Selling
- Chaves de condição para o AWS Partner Central Selling

Ações definidas pelo AWS Partner Central Selling

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar

a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptEngagementInvitation	Concede permissão para aceitar convites de engajamento no AWS Partner Central	Gravar	engagement-invitation*		
				partnercentral:Catalog	
AssignOpportunity	Concede permissão para atribuir oportunidades no AWS Partner Central	Gravar	Opportunity*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				partnercentral:Catalog	
AssociateOpportunity	Concede permissão para associar oportunidades no AWS Partner Central a outras entidades	Gravar	Opportunity*		
				partnercentral:Catalog partnercentral:RelatedEntityType	
CreateEngagement	Concede permissão para criar engajamentos no AWS Partner Central	Gravar	Engagement*		
				partnercentral:Catalog	
CreateEngagementInvitation	Concede permissão para criar convites de engajamento no AWS Partner Central	Gravar	engagement-invitation*		
				partnercentral:Catalog	
CreateOpportunity	Concede permissão para criar novas oportunidades no AWS Partner Central	Gravar	Opportunity*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys partnercentral:Catalog	
CreateResourceSnapshot	Concede permissão para criar instantâneos de recursos no AWS Partner Central	Gravar	ResourceSnapshot*		
				partnercentral:Catalog	
CreateResourceSnapshotJob	Concede permissão para criar trabalhos de instantâneos de recursos no AWS Partner Central	Gravar	resource-snapshot-job*		
				aws:RequestTag/${TagKey} aws:TagKeys partnercentral:Catalog	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteResourceSnapshotJob	Concede permissão para excluir trabalhos de instantâneos de recursos no AWS Partner Central	Gravar	resource-snapshot-job*		
				partnercentral:Catalog	
DisassociateOpportunity	Concede permissão para desassociar oportunidades no AWS Partner Central de outras entidades	Gravar	Opportunity*		
				partnercentral:Catalog partnercentral:RelatedEntityType	
GetAwsOpportunitySummary	Concede permissão para recuperar resumos AWS de oportunidades para oportunidades no AWS Partner Central	Leitura	Opportunity*		
				partnercentral:Catalog	
GetEngagement	Concede permissão para recuperar os detalhes do engajamento no AWS Partner Central	Leitura	Engagement*		
				partnercentral:Catalog	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetEngagementInvitation	Concede permissão para recuperar detalhes dos convites de engajamento no Partner Central AWS	Leitura	engagement-invitation*		
				partnercentral:Catalog	
GetOpportunity	Concede permissão para recuperar detalhes de oportunidades no AWS Partner Central	Leitura	Opportunity*		
				partnercentral:Catalog	
GetResourceSnapshot	Concede permissão para recuperar detalhes do instantâneo do recurso no AWS Partner Central	Leitura	ResourceSnapshot*		
				partnercentral:Catalog	
GetResourceSnapshotJob	Concede permissão para recuperar detalhes do trabalho de captura instantânea de recursos no AWS Partner Central	Leitura	resource-snapshot-job*		
				partnercentral:Catalog	
GetSellingSystemSettings	Concede permissão para recuperar as configurações do sistema no AWS Partner Central	Leitura		partnercentral:Catalog	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListEngagementByAcceptingInvitationTasks	Concede permissão para listar compromissos aceitando tarefas de convite no AWS Partner Central	Lista		partnercentral:Catalog	
ListEngagementFromOpportunityTasks	Concede permissão para listar engajamentos de tarefas de oportunidade no AWS Partner Central	Lista		partnercentral:Catalog	
ListEngagementInvitations	Concede permissão para listar convites de engajamento no AWS Partner Central	Lista		partnercentral:Catalog	
ListEngagementMembers	Concede permissão para listar membros do engajamento no AWS Partner Central	Leitura	Engagement*		
				partnercentral:Catalog	
ListEngagementResourceAssociations	Concede permissão para listar associações de recursos de engajamento no AWS Partner Central	Leitura	ResourceSnapshot*		
				partnercentral:Catalog	
ListEngagements	Concede permissão para listar compromissos no AWS Partner Central	Lista		partnercentral:Catalog	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListOpportunities	Concede permissão para listar oportunidades no AWS Partner Central	Lista		partnercentral:Catalog	
ListResourceSnapshotJobs	Concede permissão para listar trabalhos de instantâneos de recursos no AWS Partner Central	Lista		partnercentral:Catalog	
ListResourceSnapshots	Concede permissão para listar instantâneos de recursos no AWS Partner Central	Leitura	ResourceSnapshot*		
				partnercentral:Catalog	
ListSolutions	Concede permissão para listar soluções no AWS Partner Central	Lista		partnercentral:Catalog	
ListTagsForResource	Concede permissão para adicionar tags de listas a um recurso. Recurso suportado: ResourceSnapshotJob	Leitura		aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutSellingSystemSettings	Concede permissão para colocar as configurações do sistema no AWS Partner Central	Gravar			
RejectEngagementInvitation	Concede permissão para rejeitar convites de engajamento no AWS Partner Central	Gravar	engagement-invitation*		
				partnercentral:Catalog	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartEngagementByAcceptingInvitationTask	Concede permissão para iniciar tarefas que iniciam engajamentos no AWS Partner Central aceitando um convite de engajamento	Gravar	engagement-by-accepting-invitation-task*		partnercentral:AcceptEngagementInvitation partnercentral:CreateOpportunity partnercentral:CreateResourceSnapshotJob partnercentral:GetEngagementInvitation partnercentral:StartResourceSnapshotJob partnercentral:SubmitOpportunity

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartEngagementFromOpportunityTask	Concede permissão para iniciar tarefas que iniciam engajamentos a partir de oportunidades no Partner Central AWS	Gravar	engagement-from-opportunity-task*		partnercentral:CreateEngagement partnercentral:CreateEngagementInvitation partnercentral:CreateResourceSnapshotJob partnercentral:GetOpportunity partnercentral:StartResourceSnapshotJob partnercentral:SubmitOpportunity

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	
StartResourceSnapshotJob	Concede permissão para iniciar trabalhos de instantâneos de recursos no AWS Partner Central	Gravar	resource-snapshot-job*		
				partnercentral:Catalog	
StopResourceSnapshotJob	Concede permissão para interromper trabalhos de captura de tela de recursos no AWS Partner Central	Gravar	resource-snapshot-job*		
				partnercentral:Catalog	
SubmitOpportunity	Concede permissão para enviar oportunidades no AWS Partner Central	Gravar	Opportunity*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				partnercentral:Catalog	
TagResource	Concede permissão para adicionar novas tags a um recurso. Recurso suportado: ResourceSnapshotJob	Tags	Opportunity		
			resource-snapshot-job		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	
UntagResource	Concede permissão para remover tags de um recurso. Recurso suportado: ResourceSnapshotJob	Tags	Opportunity		
			resource-snapshot-job		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	
UpdateOpportunity	Concede permissão para atualizar oportunidades no AWS Partner Central	Gravar	Opportunity*		
				partnercentral:Catalog	

Tipos de recursos definidos pelo AWS Partner Central Selling

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}	
Opportunity	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/opportunity/${Identifier}	aws:ResourceTag/${TagKey}
resource-snapshot-job	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/resource-snapshot-job/${Identifier}	aws:ResourceTag/${TagKey}
ResourceSnapshot	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/engagement/${EngagementIdentifier}/resource/${ResourceType}/${ResourceIdentifier}/template/${TemplateIdentifier}/resource-snapshot/${SnapshotRevision}	

Tipos de recursos	ARN	Chaves de condição
Solution	`arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/solution/${Identifier}`	

Chaves de condição para o AWS Partner Central Selling

AWS O Partner Central Selling define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString
partnercentral:Catalog	Filtra o acesso por um catálogo específico. Valores aceitos: [AWS, Sandbox]	String
partnercentral:RelatedEntityType	Filtra o acesso por tipos de entidade para associação de oportunidades. Valores aceitos: [Soluções, AwsProducts, AwsMarketplaceOffers]	String

Ações, recursos e chaves de condição para Criptografia de Pagamento da AWS

AWS A criptografia de pagamento (prefixo do serviço:`payment-cryptography`) fornece os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Criptografia de Pagamento da AWS
- Tipos de recursos definidos pela Criptografia de Pagamento da AWS
- Chaves de condição para a Criptografia de Pagamento da AWS

Ações definidas pela Criptografia de Pagamento da AWS

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar

a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAlias	Concede permissão para criar um nome fácil de usar para uma chave	Gravar	alias*		
			key*		
CreateKey	Concede permissão para criar uma chave exclusiva gerenciada pelo cliente no chamador Conta da AWS e na região	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	payment-cryptography:TagResource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DecryptData	Concede permissão para descriptografar dados de texto cifrado em texto simples usando chave de criptografia de dados simétrica, assimétrica ou DUKPT	Gravar	alias*		
			key*		
DeleteAlias	Concede permissão para excluir o alias da especificada	Gravar	alias*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteKey	Concede permissão para programar a exclusão de uma chave	Gravar	key*		
EncryptData	Concede permissão para criptografar dados de texto simples em texto cifrado usando chave de criptografia de dados simétrica, assimétrica ou DUKPT	Gravar	alias*		
			key*		
ExportKey	Concede permissão para exportar uma chave do serviço	Gravar	key*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GenerateCardValidationData	Concede permissão para gerar dados relacionados ao cartão usando algoritmos como Card Verification Values (CVV/CVV2), Dynamic Card Verification Values (dCVV/dCVV2) ou Card Security Codes (CSC) que verificam a validade de um cartão com tarja magnética	Gravar	alias*		
			key*		
GenerateMac	Concede permissão para gerar um criptograma de MAC (código de autenticação de mensagens)	Gravar	alias*		
			key*		
GenerateMacEmvPinChange	Concede permissão para gerar um criptograma de MAC (código de autenticação de mensagens)	Gravar	alias*		
			key*		
GeneratePinData	Concede permissão para gerar dados relacionados ao PIN, como PIN, valor de verificação de PIN (PVV), bloqueio de PIN e compensação de PIN durante a emissão ou reemissão de um novo cartão	Gravar	alias*		
			key*		
GetAlias	Concede permissão para retornar o keyArn associado a um aliasName	Leitura	alias*		
			key*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
GetKey	Concede permissão para retornar informações detalhadas sobre a chave especificada	Leitura	key*		
GetParametersForExport	Concede permissão para obter o token de exportação e o certificado da chave de assinatura para iniciar uma exportação de chave TR-34	Leitura			
GetParametersForImport	Concede permissão para obter o token de importação e o certificado da chave de empacotamento para iniciar uma importação de chave TR-34	Leitura			
GetPublicKeyCertificate	Concede permissão para retornar a chave pública de uma chave da classe PUBLIC_KEY	Leitura	key*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ImportKey	Concede permissão para importar chaves e certificados de chave pública	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	payment-cryptography:TagResource
ListAliases	Concede permissão para retornar uma lista de aliases criados para todas as chaves no chamador e na região Conta da AWS	Lista			
ListKeys	Concede permissão para retornar uma lista de chaves criadas no chamador Conta da AWS e na região	Lista			
ListTagsForResource	Concede permissão para retornar uma lista de tags criadas no chamador Conta da AWS e na região	Leitura	key		
ReEncryptData	Concede permissão para criptografar novamente dados de texto cifrado usando DUKPT e chaves de criptografia de dados simétricas e assimétricas	Gravar	alias* key*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RestoreKey	Concede permissão para cancelar uma exclusão programada de chave se, em algum momento durante o período de espera, uma chave precisar ser reativada	Gravar	key*		
StartKeyUsage	Concede permissão para ativar uma chave desativada	Gravar	key*		
StopKeyUsage	Concede permissão para desativar uma chave ativada	Gravar	key*		
TagResource	Concede permissão para adicionar ou substituir uma ou mais tags do recurso especificado	Tags	key*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TranslatePinData	Concede permissão para traduzir o bloco PIN criptografado de e para os formatos ISO 9564 0,1,3,4	Gravar	alias*		
			key*		
UntagResource	Concede permissão para remover a tag ou as tags especificadas do recurso especificado	Tags	key*		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateAlias	Concede permissão para alterar a chave à qual um alias está atribuído ou cancelar sua atribuição da chave atual	Gravar	alias*		
			key*		
				aws:RequestTag/${TagKey} aws:TagKeys	
VerifyAuthRequestCryptogram	Concede permissão para verificar o criptograma de solicitação de autorização (ARQC) para uma autorização de cartão de pagamento com chip EMV	Gravar	alias*		
			key*		
VerifyCardValidationData	Concede permissão para verificar dados de validação relacionados ao cartão usando algoritmos como Card Verification Values (CVV/CVV2), Dynamic Card Verification Values (dCVV/dCVV2) e Card Security Codes (CSC)	Gravar	alias*		
			key*		
VerifyMac	Concede permissão para verificar o MAC (código de autenticação de mensagens) dos dados de entrada em relação a um MAC fornecido	Gravar	alias*		
			key*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
VerifyPinData	Concede permissão para verificar dados relacionados a PIN, como PIN e PIN Offset, usando algoritmos como VISA PVV e IBM3624	Gravar	alias*		
			key*		

Tipos de recursos definidos pela Criptografia de Pagamento da AWS

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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

Chaves de condição para a Criptografia de Pagamento da AWS

AWS A criptografia de pagamento define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pela chave e valor da tag na solicitação da operação especificada	String
aws:ResourceTag/${TagKey}	Filtra o acesso por tags atribuídas a uma chave para a operação especificada	String
aws:TagKeys	Filtra o acesso pelas chaves de tag na solicitação da operação especificada	ArrayOfString
payment-cryptography:CertificateAuthorityPublicKeyIdentifier	Filtra o acesso pelo CertificateAuthorityPublicKeyIdentifier especificado na solicitação ou nas ImportKey ExportKey operações e	String
payment-cryptography:ImportKeyMaterial	Filtra o acesso pelo tipo de material chave que está sendo importado [RootCertificatePublicKey, TrustedCertificatePublicKey, Tr34KeyBlock, Tr31KeyBlock] para a operação ImportKey	String
payment-cryptography:KeyAlgorithm	Filtra o acesso por KeyAlgorithm especificado na solicitação da CreateKey operação	String

Chaves de condição	Descrição	Tipo
payment-cryptography:KeyClass	Filtra o acesso por KeyClass especificado na solicitação da CreateKey operação	String
payment-cryptography:KeyUsage	Filtra o acesso por KeyClass especificado na solicitação ou associado a uma chave para a CreateKey operação	String
payment-cryptography:RequestAlias	Filtra o acesso pelos aliases na solicitação da operação especificada	String
payment-cryptography:ResourceAliases	Filtra o acesso pelos aliases associados a uma chave da operação especificada	ArrayOfString
payment-cryptography:WrappingKeyIdentifier	Filtra o acesso pelo WrappingKeyIdentifier especificado na solicitação para as ExportKey operações ImportKey, e.	String

Ações, recursos e chaves de condição para o AWS Payments

AWS O Payments (prefixo do serviço:`payments`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Payments
- Tipos de recursos definidos pelo AWS Payments
- Chaves de condição para o AWS Payments

Ações definidas pelo AWS Payments

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de

recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptFinancingApplicationTerms	Concede permissão para aceitar os termos do pedido de financiamento fornecidos por um credor	Gravar			
CreateFinancingApplication	Concede permissão para criar um aplicativo de financiamento	Gravar			
CreatePaymentInstrument	Concede permissão para criar um instrumento de pagamento	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
DeletePaymentInstrument [somente permissão]	Concede permissão para excluir um instrumento de pagamento	Gravar			
GetFinancingApplication	Concede permissão para obter informações sobre um pedido de financiamento	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetFinancingLine	Concede permissão para obter informações sobre uma linha de financiamento	Leitura			
GetFinancingLineWithdrawal	Concede permissão para obter informações sobre a retirada de uma linha de financiamento	Leitura			
GetFinancingOption	Concede permissão para obter informações sobre uma opção de financiamento	Leitura			
GetPaymentInstrument	Concede permissão para obter informações sobre um instrumento de pagamento	Lista	payment-instrument		
GetPaymentStatus [somente permissão]	Concede permissão para obter o status de pagamento de faturas	Leitura			
ListFinancingApplications	Concede permissão para listar os metadados do aplicativo de financiamento	Lista			
ListFinancingLineWithdrawals	Concede permissão para listar metadados de saques de linhas de financiamento	Lista			
ListFinancingLines	Concede permissão para listar metadados da linha de financiamento	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListPaymentInstruments [somente permissão]	Concede permissão para listar metadados de instrumentos de pagamento	Lista			
ListPaymentPreferences [somente permissão]	Concede permissão para obter preferências de pagamento (moeda preferencial de pagamento, método preferencial de pagamento etc.)	Lista			
ListPaymentProgramOptions	Concede permissão para listar informações sobre as opções de pagamento	Lista			
ListPaymentProgramStatus	Concede permissão para listar informações sobre elegibilidade do programa de pagamento e status de inscrição	Lista			
ListTagsForResource	Concede permissão para listar tags em um recurso de pagamento	Lista	payment-instrument		
MakePayment [somente permissão]	Concede permissão para fazer um pagamento, autenticar um pagamento, verificar uma forma de pagamento e gerar um documento de solicitação de financiamento para pagamento antecipado	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para marcar um recurso de pagamento	Tags	payment-instrument		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para desmarcar um recurso de pagamento	Tags	payment-instrument		
				aws:TagKeys	
UpdateFinancingApplication	Concede permissão para atualizar um pedido de financiamento	Gravar			
UpdatePaymentInstrument [somente permissão]	Concede permissão para atualizar um instrumento de pagamento	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdatePaymentPreferences [somente permissão]	Concede permissão para atualizar preferências de pagamento (moeda preferencial de pagamento, método preferencial de pagamento etc.)	Gravar			

Tipos de recursos definidos pelo AWS Payments

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
payment-instrument	`arn:${Partition}:payments::${Account}:payment-instrument:${ResourceId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o AWS Payments

AWS O Payments define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Performance Insights

AWS O Performance Insights (prefixo do serviço:`pi`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Performance Insights
- Tipos de recursos definidos pelo AWS Performance Insights
- Chaves de condição do AWS Performance Insights

Ações definidas pelo AWS Performance Insights

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreatePerformanceAnalysisReport	Concede permissão para chamar a CreatePerformanceAnalysisReport API para criar um relatório de análise de desempenho para uma instância de banco de dados especificada	Gravar	perf-reports-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeletePerformanceAnalysisReport	Concede permissão para chamar a DeletePerformanceAnalysisReport API para excluir um relatório de análise de desempenho para uma instância de banco de dados especificada	Gravar	perf-reports-resource*		
DescribeDimensionKeys	Concede permissão para chamar a DescribeDimensionKeys API para recuperar as N principais chaves de dimensão de uma métrica em um período específico	Leitura	metric-resource*		
				pi:Dimensions	
GetDimensionKeyDetails	Concede permissão para chamar a GetDimensionKeyDetails API para recuperar os atributos do	Leitura	metric-resource*		
				pi:Dimensions	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	grupo de dimensões especificado				
GetPerformanceAnalysisReport	Concede permissão para chamar a GetPerformanceAnalysisReport API para recuperar um relatório de análise de desempenho para uma instância de banco de dados especificada	Leitura	perf-reports-resource*		
GetResourceMetadata	Concede permissão para chamar a GetResourceMetadata API para recuperar os metadados de diferentes recursos	Leitura	metric-resource*		
GetResourceMetrics	Concede permissão para chamar a GetResourceMetrics API para recuperar métricas de PI para um conjunto de fontes de dados, durante um período de tempo	Leitura	metric-resource*		
				pi:Dimensions	
ListAvailableResourceDimensions	Concede permissão para chamar a ListAvailableResourceDimensions API para recuperar as dimensões que podem ser consultadas para cada tipo de métrica especificado em uma instância de banco de dados especificada	Leitura	metric-resource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAvailableResourceMetrics	Concede permissão para chamar a ListAvailableResourceMetrics API para recuperar métricas dos tipos especificados que podem ser consultadas para uma instância de banco de dados especificada	Leitura	metric-resource*		
ListPerformanceAnalysisReports	Concede permissão para chamar a ListPerformanceAnalysisReports API para listar relatórios de análise de desempenho para uma instância de banco de dados especificada	Lista	perf-reports-resource*		
ListTagsForResource	Concede permissão para chamar a ListTagsForResource API para listar tags para um recurso	Lista	perf-reports-resource*		
TagResource	Concede permissão para chamar a TagResource API para marcar um recurso	Tags	perf-reports-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para chamar a UntagResource API para desmarcar um recurso	Tags	perf-reports-resource*		
				aws:TagKeys	

Tipos de recursos definidos pelo AWS Performance Insights

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS Performance Insights

AWS O Performance Insights define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais

as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString
pi:Dimensions	Filtra o acesso pelas dimensões solicitadas	ArrayOfString

Ações, recursos e chaves de condição do Amazon Personalize

O Amazon Personalize (prefixo do serviço: `personalize`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Personalize
- Tipos de recursos definidos pelo Amazon Personalize
- Chaves de condição do Amazon Personalize

Ações definidas pelo Amazon Personalize

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateBatchInferenceJob	Concede permissão para criar um trabalho de inferência em lote	Gravar	batchInferenceJob*		
CreateBatchSegmentJob	Concede permissão para criar um trabalho de segmento em lote	Gravar	batchSegmentJob*		
CreateCampaign	Concede permissão para criar uma campanha	Gravar	campaign*		
CreateDataDeletionJob	Concede permissão para criar um trabalho de exclusão de dados	Gravar	dataDeletionJob*		
CreateDataInsightsJob	Concede permissão para criar um trabalho de insights de dados	Gravar	dataInsightsJob*		
CreateDataset	Concede permissão para criar um conjunto de dados	Gravar	dataset*		
CreateDatasetExportJob	Concede permissão para criar um trabalho de exportação de conjunto de dados	Gravar	datasetExportJob*		
CreateDatasetGroup	Concede permissão para criar um grupo de conjuntos de dados	Write	datasetGroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDatasetImportJob	Concede permissão para criar um trabalho de importação de conjunto de dados	Write	datasetImportJob*		
CreateEventTracker	Concede permissão para criar um rastreador de eventos	Write	eventTracker*		
CreateFilter	Concede permissão para criar um filtro	Gravar	filter*		
CreateMetricAttribution	Concede permissão para criar uma atribuição de métricas	Gravar	metricAttribution*		
CreateRecommender	Concede permissão para criar um recomendador	Gravar	recommender*		
CreateSchema	Concede permissão para criar um esquema	Write	schema*		
CreateSolution	Concede permissão para criar uma solução	Write	solution*		
CreateSolutionVersion	Concede permissão para criar uma versão da solução	Write	solution*		
DeleteCampaign	Concede permissão para excluir uma campanha	Write	campaign*		
DeleteDataset	Concede permissão para excluir um conjunto de dados	Write	dataset*		
DeleteDatasetGroup	Concede permissão para excluir um grupo de conjuntos de dados	Write	datasetGroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteEventTracker	Concede permissão para excluir um rastreador de eventos	Write	eventTracker*		
DeleteFilter	Concede permissão para excluir um filtro	Gravar	filter*		
DeleteMetricAttribution	Concede permissão para excluir uma atribuição de métricas	Gravar	metricAttribution*		
DeleteRecommender	Concede permissão para excluir um recomendador	Gravar	recommender*		
DeleteSchema	Concede permissão para excluir um esquema	Write	schema*		
DeleteSolution	Concede permissão para excluir uma solução, incluindo todas as versões da solução	Write	solution*		
DescribeAlgorithm	Concede permissão para descrever um algoritmo	Read	algorithm*		
DescribeBatchInferenceJob	Concede permissão para descrever um trabalho de inferência em lote	Leitura	batchInferenceJob*		
DescribeBatchSegmentJob	Concede permissão para descrever um trabalho de segmento em lote	Leitura	batchSegmentJob*		
DescribeCampaign	Concede permissão para descrever uma campanha	Leitura	campaign*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeDataDeletionJob	Concede permissão para descrever um trabalho de exclusão de dados	Leitura	dataDeletionJob*		
DescribeDataInsightsJob	Concede permissão para descrever um trabalho de insights de dados	Leitura	dataInsightsJob*		
DescribeDataset	Concede permissão para descrever um conjunto de dados	Leitura	dataset*		
DescribeDatasetExportJob	Concede permissão para descrever um trabalho de exportação de conjunto de dados	Leitura	datasetExportJob*		
DescribeDatasetGroup	Concede permissão para descrever um grupo de conjuntos de dados	Read	datasetGroup*		
DescribeDatasetImportJob	Concede permissão para descrever um trabalho de importação de conjunto de dados	Read	datasetImportJob*		
DescribeEventTracker	Concede permissão para descrever um rastreador de eventos	Read	eventTracker*		
DescribeFeatureTransformation	Concede permissão para descrever uma transformação de recurso	Read	featureTransformation*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeFilter	Concede permissão para descrever um filtro	Leitura	filter*		
DescribeMetricAttribution	Concede permissão para descrever uma atribuição de métricas	Leitura	metricAttribution*		
DescribeRecipe	Concede permissão para descrever uma receita	Leitura	recipe*		
DescribeRecommender	Concede permissão para descrever uma recomendação	Leitura	recommender*		
DescribeSchema	Concede permissão para descrever um esquema	Read	schema*		
DescribeSolution	Concede permissão para descrever uma solução	Read	solution*		
DescribeSolutionVersion	Concede permissão para descrever uma versão de uma solução	Leitura	solution*		
GetActionRecommendations	Concede permissão para obter uma lista de ações recomendadas	Leitura	campaign*		
GetDataInsights	Concede permissão para obter insights de dados de um trabalho de insights de dados	Leitura	dataInsightsJob*		
GetPersonalizedRanking	Concede permissão para obter uma lista reclassificada de recomendações	Read	campaign*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetRecommendations	Concede permissão para obter uma lista de recomendações de uma campanha	Read	campaign*		
GetSolutionMetrics	Concede permissão para obter métricas para uma versão da solução	Read	solution*		
ListBatchInferenceJobs	Concede permissão para listar trabalhos de inferência em lote	Lista			
ListBatchSegmentJobs	Concede permissão para listar lotes de trabalhos de segmento	Lista			
ListCampaigns	Concede permissão para listar campanhas	Lista			
ListDataDeletionJobs	Concede permissão para listar trabalhos de exclusão de dados	Lista			
ListDataInsightsJobs	Concede permissão para listar trabalhos de insights de dados	Lista			
ListDatasetExportJobs	Concede permissão para listar trabalhos de exportação do conjunto de dados	Lista			
ListDatasetGroups	Concede permissão para listar grupos de conjuntos de dados	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDatasetImportJobs	Concede permissão para listar trabalhos de importação do conjunto de dados	List			
ListDatasets	Concede permissão para listar conjuntos de dados	List			
ListEventTrackers	Concede permissão para listar rastreadores de eventos	List			
ListFilters	Concede permissão para listar filtros	Lista			
ListMetricAttributionMetrics	Concede permissão para listar métricas de atribuição de métricas	Lista			
ListMetricAttributions	Concede permissão para listar atribuições de métricas	Lista			
ListRecipes	Concede permissão para listar receitas	Lista			
ListRecommenders	Concede permissão para listar recomendações	Lista			
ListSchemas	Concede permissão para listar esquemas	List			
ListSolutionVersions	Concede permissão para listar versões de uma solução	List			
ListSolutions	Concede permissão para listar soluções	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Lista			
PutActionInteractions	Concede permissão para adicionar dados de interação de ações em tempo real	Gravar			
PutActions	Concede permissão para ingerir dados de ações	Gravar	dataset*		
PutEvents	Concede permissão para colocar dados de eventos em tempo real	Write			
PutItems	Concede permissão para ingerir dados de itens	Write	dataset*		
PutUsers	Concede permissão para ingerir dados de usuários	Gravar	dataset*		
StartRecommender	Concede permissão para iniciar um recomendador	Gravar	recommender*		
StopRecommender	Concede permissão para interromper um recomendador	Gravar	recommender*		
StopSolutionVersionCreation	Concede permissão para interromper uma versão da solução	Gravar	solution*		
TagResource	Concede permissão para marcar um recurso	Marcação			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para desmarcar um recurso	Tags			
UpdateCampaign	Concede permissão para atualizar uma campanha	Gravar	campaign*		
UpdateDataset	Concede permissão para atualizar um conjunto de dados	Gravar	dataset*		
UpdateMetricAttribution	Concede permissão para atualizar uma atribuição de métricas	Gravar	metricAttribution*		
UpdateRecommender	Concede permissão para atualizar uma recomendação	Gravar	recommender*		
UpdateSolution	Concede permissão para atualizar uma solução	Gravar	solution*		

Tipos de recursos definidos pelo Amazon Personalize

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}	
campaign	arn:${Partition}:personalize:${Region}:${Account}:campaign/${ResourceId}	

Tipos de recursos	ARN	Chaves de condição
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}	

Chaves de condição do Amazon Personalize

O Personalize não possui chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do Amazon Pinpoint

O Amazon Pinpoint (prefixo do serviço: `mobiletargeting`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Pinpoint
- Tipos de recursos definidos pelo Amazon Pinpoint
- Chaves de condição do Amazon Pinpoint

Ações definidas pelo Amazon Pinpoint

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateApp	Concede permissão para criar uma aplicação	Gravar	apps*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateCampaign	Concede permissão para criar uma campanha para uma aplicação	Gravar	app*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateEmailTemplate	Concede permissão para criar um modelo de e-mail	Gravar	template*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateExportJob	Concede permissão para criar um trabalho que exporta definições de endpoint para o Amazon S3	Gravar	app*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateImportJob	Concede permissão para importar definições de endpoint a partir da criação de um segmento	Gravar	app*		
CreateInAppTemplate	Concede permissão para criar um modelo de mensagem in-app	Gravar	template*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateJourney	Concede permissão para criar uma jornada para uma aplicação	Gravar	journeys*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreatePushTemplate	Concede permissão para criar um modelo de notificação por push	Gravar	template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateRecommenderConfiguration	Concede permissão para criar uma configuração do Amazon Pinpoint para um modelo de recomendação	Gravar	recommenders*		
CreateSegment	Concede permissão para criar um segmento baseado em dados de endpoint relatados ao Pinpoint por sua aplicação. Para permitir que um usuário crie um segmento importando dados de endpoint de fora do Pinpoint, permita a ação mobiletargeting: CreateImportJob	Gravar	app*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateSmsTemplate	Concede permissão para criar um modelo de mensagem sms	Gravar	template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateVoiceTemplate	Concede permissão para criar um modelo de mensagem de voz	Gravar	template*	aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeleteAdmChannel	Concede permissão para excluir o canal ADM de uma aplicação	Gravar	channel*		
DeleteApnsChannel	Concede permissão para excluir o APNs canal de um aplicativo	Gravar	channel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteApnsSandboxChannel	Concede permissão para excluir o canal APNs sandbox de um aplicativo	Gravar	channel*		
DeleteApnsVoipChannel	Concede permissão para excluir o canal APNs VoIP de um aplicativo	Gravar	channel*		
DeleteApnsVoipSandboxChannel	Concede permissão para excluir o canal de sandbox de APNs VoIP de um aplicativo	Gravar	channel*		
DeleteApp	Concede permissão para excluir uma campanha específica	Gravar	app*		
DeleteBaiduChannel	Concede permissão para excluir o canal Baidu de uma aplicação	Gravar	channel*		
DeleteCampaign	Concede permissão para excluir uma campanha específica	Gravar	campaign*		
DeleteEmailChannel	Concede permissão para excluir o canal de e-mail para uma aplicação	Gravar	channel*		
DeleteEmailTemplate	Concede permissão para excluir um modelo de e-mail ou uma versão do modelo de e-mail	Gravar	template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteEndpoint	Concede permissão para excluir um endpoint	Gravar	endpoint*		
DeleteEventStream	Concede permissão para excluir a transmissão de eventos de uma aplicação	Gravar	event-stream*		
DeleteGcmChannel	Concede permissão para excluir o canal GCM de uma aplicação	Gravar	channel*		
DeleteInAppTemplate	Concede permissão para excluir um modelo de mensagem in-app ou uma versão do modelo de mensagem in-app	Gravar	template*		
DeleteJourney	Concede permissão para excluir uma jornada específica	Gravar	journey*		
DeletePushTemplate	Concede permissão para excluir um modelo de notificação por push ou uma versão do modelo de notificação por push	Gravar	template*		
DeleteRecommenderConfiguration	Conceder permissão para excluir uma configuração do Amazon Pinpoint para um modelo de recomendação	Gravar	recommender*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteSegment	Concede permissão para excluir um segmento específico	Gravar	segment*		
DeleteSmsChannel	Concede permissão para excluir o canal de SMS de uma aplicação	Gravar	channel*		
DeleteSmsTemplate	Concede permissão para excluir um modelo de mensagem sms ou uma versão do modelo de mensagem sms	Gravar	template*		
DeleteUserEndpoints	Concede permissão para excluir todos os endpoints que estão associados a um ID de usuário	Gravar	user*		
DeleteVoiceChannel	Concede permissão para excluir o canal de voz para uma aplicação	Gravar	channel*		
DeleteVoiceTemplate	Concede permissão para excluir um modelo de mensagem de voz ou uma versão do modelo de mensagem de voz	Gravar	template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAdmChannel	Concede permissão para recuperar informações sobre o canal Amazon Device Messaging (ADM) para uma aplicação	Leitura	channel*		
GetApnsChannel	Concede permissão para recuperar informações sobre o APNs canal de um aplicativo	Leitura	channel*		
GetApnsSandboxChannel	Concede permissão para recuperar informações sobre o canal APNs sandbox de um aplicativo	Leitura	channel*		
GetApnsVoipChannel	Concede permissão para recuperar informações sobre o canal APNs VoIP de um aplicativo	Leitura	channel*		
GetApnsVoipSandboxChannel	Concede permissão para recuperar informações sobre o canal de sandbox de APNs VoIP para um aplicativo	Leitura	channel*		
GetApp	Conceder permissão para recuperar informações sobre uma aplicação específica em sua conta do Amazon Pinpoint	Leitura	app*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetApplicationDateRangeKpi	Conceder permissão para recuperar (filas) dados pré-agregados para uma métrica padrão que se aplica a uma aplicação	Leitura	application-metrics*		
GetApplicationSettings	Concede permissão para recuperar as configurações padrão de uma aplicação	Lista	app*		
GetApps	Concede permissão para recuperar uma lista de aplicações em sua conta do Amazon Pinpoint	Leitura	apps*		
GetBaiduChannel	Concede permissão para recuperar informações sobre o canal Baidu para uma aplicação	Leitura	channel*		
GetCampaign	Concede permissão para recuperar informações sobre uma campanha específica	Leitura	campaign*		
GetCampaignActivities	Concede permissão para recuperar informações sobre as atividades executadas por uma campanha	Lista	campaign*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetCampaignDateRangeKpi	Conceder permissão para recuperar (filas) dados pré-agregados para uma métrica padrão que se aplica a uma campanha	Leitura	campaign-metrics*		
GetCampaignVersion	Concede permissão para recuperar informações sobre uma versão de campanha específica	Leitura	campaign*		
GetCampaignVersions	Concede permissão para recuperar informações sobre as versões atual e anterior de uma campanha	Lista	campaign*		
GetCampaigns	Concede permissão para recuperar informações sobre todas as campanhas para uma aplicação	Lista	app*		
GetChannels	Concede permissão para obter as informações de todos os canais de sua aplicação	Lista	channels*		
GetEmailChannel	Concede permissão para obter informações sobre o canal de e-mail em uma aplicação	Leitura	channel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetEmailTemplate	Concede permissão para recuperar informações sobre uma versão específica ou ativa de um modelo de e-mail	Leitura	template*		
GetEndpoint	Concede permissão para recuperar informações sobre um endpoint específico	Leitura	endpoint*		
GetEventStream	Concede permissão para recuperar informações sobre a sequência de eventos para uma aplicação	Leitura	event-stream*		
GetExportJob	Concede permissão para obter informações sobre um trabalho de exportação específico	Leitura	export-job*		
GetExportJobs	Concede permissão para recuperar uma lista de todos trabalhos de exportação de uma aplicação	Lista	app*		
GetGcmChannel	Concede permissão para recuperar informações sobre o canal GCM para uma aplicação	Leitura	channel*		
GetImportJob	Concede permissão para recuperar informações sobre um trabalho de importação específico	Leitura	import-job*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetImportJobs	Concede permissão para recuperar informações sobre todas os trabalhos de importação para uma aplicação	Lista	app*		
GetInAppMessages	Concede permissão para recuperar mensagens na aplicação para o ID do endpoint fornecido	Leitura	app*		
GetInAppTemplate	Concede permissão para recuperar informações sobre uma versão específica ou ativa de um modelo de mensagem in-app	Leitura	template*		
GetJourney	Concede permissão para recuperar informações sobre uma jornada específica	Leitura	journey*		
GetJourneyDateRangeKpi	Concede permissões para recuperar (consultas) dados pré-agregados para uma métrica de engajamento padrão que se aplica a uma jornada	Leitura	journey-metrics*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetJourneyExecutionActivityMetrics	Concede permissão para recuperar (consultas) dados pré-agregados para uma métrica de execução padrão que se aplica a uma atividade de jornada	Leitura	journey-execution-activity-metrics*		
GetJourneyExecutionMetrics	Concede permissão para recuperar (consultas) dados pré-agregados para uma métrica de execução padrão que se aplica a uma jornada	Leitura	journey-execution-metrics*		
GetJourneyRunExecutionActivityMetrics	Concede permissão para recuperar (consultas) dados pré-agregados para uma métrica de execução padrão que se aplica a uma atividade de jornada para uma única execução de jornada	Leitura	journey*		
GetJourneyRunExecutionMetrics	Concede permissão para recuperar (consultas) dados pré-agregados para uma métrica de execução padrão que se aplica a uma jornada para uma única execução de jornada	Leitura	journey*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetJourneyRuns	Concede permissão para recuperar informações sobre todas as execuções de jornadas de uma jornada	Lista	journey*		
GetPushTemplate	Concede permissão para recuperar informações sobre uma versão específica ou ativa de um modelo de notificação por push	Leitura	template*		
GetRecommenderConfiguration	Concede permissão para recuperar informações sobre uma configuração do Amazon Pinpoint para um modelo de recomendação	Leitura	recommender*		
GetRecommenderConfigurations	Concede permissão para recuperar informações sobre todas as configurações de modelo de recomendação associadas a uma conta do Amazon Pinpoint	Lista	recommenders*		
GetReports [somente permissão]	Concede permissão à segmentação móvel: GetReports	Leitura	reports*		
GetSegment	Concede permissão para recuperar informações sobre um segmento específico	Leitura	segment*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSegmentExportJobs	Conceder permissão para recuperar informações sobre trabalhos que exportam definições de endpoint de segmentos para o Amazon S3	Lista	segment*		
GetSegmentImportJobs	Concede permissão para recuperar informações sobre trabalhos que criem segmentos importando definições de endpoint de	Lista	segment*		
GetSegmentVersion	Concede permissão para recuperar informações sobre uma versão de segmento específico	Leitura	segment*		
GetSegmentVersions	Concede permissão para recuperar informações sobre as versões atual e anterior de um segmento	Lista	segment*		
GetSegments	Concede permissão para recuperar informações sobre os segmentos de uma aplicação	Lista	app*		
GetSmsChannel	Concede permissão para obter informações sobre o canal de SMS em uma aplicação	Leitura	channel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSmsTemplate	Concede permissão para recuperar informações sobre uma versão específica ou ativa de um modelo de mensagem SMS	Leitura	template*		
GetUserEndpoints	Concede permissão para recuperar informações sobre os endpoints que estão associados a um ID de usuário	Leitura	user*		
GetVoiceChannel	Concede permissão para obter informações sobre o canal de voz em uma aplicação	Leitura	channel*		
GetVoiceTemplate	Concede permissão para recuperar informações sobre uma versão específica ou ativa de um modelo de mensagem de voz	Leitura	template*		
ListJourneys	Concede permissão para recuperar informações sobre todas as jornadas de uma aplicação	Lista	app*		
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	app		
			campaign		
			journey		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			segment		
			template		
ListTemplateVersions	Concede permissão para recuperar todas as versões de um modelo específico	Lista	template*		
ListTemplates	Concede permissão para recuperar metadados sobre modelos consultados	Lista	templates*		
PhoneNumberValidate	Concede permissão para obter metadados para um número de telefone, como o tipo de número (móvel, fixo ou VoIP), local e provedor	Leitura	phone-number-validate*		
PutEventStream	Concede permissão para criar ou atualizar uma sequência de eventos para uma aplicação	Gravar	event-stream*		
PutEvents	Concede permissão para criar ou atualizar eventos para uma aplicação	Gravar	events*		
RemoveAttributes	Concede permissão para remover os atributos de uma aplicação	Gravar	attribute*		
SendMessages	Concede permissão para enviar uma mensagem SMS ou notificação por push para endpoints específicos	Gravar	messages*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SendOTPMessage	Concede permissão para enviar um código OTP a um usuário da aplicação	Gravar	otp*		
SendUsersMessages	Concede permissão para enviar uma mensagem SMS ou notificação por push para todos os endpoints que estão associados a um ID de usuário específico	Gravar	messages*		
TagResource	Concede permissão para adicionar tags a um recurso	Marcação	app		
			campaign		
			journey		
			segment		
			template		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover etiquetas de um recurso	Tags	app		
			campaign		
			journey		
			segment		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			template		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateAdmChannel	Concede permissão para atualizar o canal do sistema de mensagens Amazon Device Messaging (ADM) de uma aplicação	Gravar	channel*		
UpdateApnsChannel	Concede permissão para atualizar o canal do serviço Apple Push Notification (APNs) para um aplicativo	Gravar	channel*		
UpdateApnsSandboxChannel	Concede permissão para atualizar o canal sandbox do serviço Apple Push Notification (APNs) para um aplicativo	Gravar	channel*		
UpdateApnsVoipChannel	Concede permissão para atualizar o canal VoIP do serviço Apple Push Notification (APNs) para um aplicativo	Gravar	channel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateApnsVoipSandboxChannel	Concede permissão para atualizar o canal sandbox de VoIP do serviço Apple Push Notification (APNs) para um aplicativo	Gravar	channel*		
UpdateApplicationSettings	Concede permissão para atualizar as configurações padrão de uma aplicação	Gravar	app*		
UpdateBaiduChannel	Concede permissão para atualizar o canal Baidu para uma aplicação	Gravar	channel*		
UpdateCampaign	Concede permissão para atualizar uma campanha específica	Gravar	campaign*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateEmailChannel	Concede permissão para atualizar o canal de e-mail para uma aplicação	Gravar	channel*		
UpdateEmailTemplate	Concede permissão para atualizar um modelo de e-mail específico da mesma versão ou gerar uma nova versão	Gravar	template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateEndpoint	Concede permissão para criar um endpoint ou atualizar as informações de um endpoint	Gravar	endpoint*		
UpdateEndpointsBatch	Conceder permissão para criar ou atualizar endpoints como uma operação em lote	Gravar	app*		
UpdateGcmChannel	Conceder permissão para atualizar a chave da API do Firebase Cloud Messaging (FCM) ou do Google Cloud Messaging (GCM) que permite enviar notificações por push à sua aplicação Android	Gravar	channel*		
UpdateInAppTemplate	Concede permissão para atualizar um modelo de mensagem in-app específico da mesma versão ou gerar uma nova versão	Gravar	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateJourney		Gravar	journey*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	Concede permissão para atualizar uma jornada específica			aws:RequestTag/${TagKey} aws:TagKeys	
UpdateJourneyState	Concede permissão para atualizar um estado de jornada específico	Gravar	journey*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdatePushTemplate	Concede permissão para atualizar um modelo de notificação por push específico da mesma versão ou gerar uma nova versão	Gravar	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateRecommenderConfiguration	Concede permissão para atualizar uma configuração do Amazon Pinpoint para um modelo de recomendação	Gravar	recommender*		
UpdateSegment	Concede permissão para atualizar um segmento específico	Gravar	segment*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateSmsChannel	Concede permissão para atualizar o canal de SMS de aplicação	Gravar	channel*		
UpdateSmsTemplate	Concede permissão para atualizar um modelo de mensagem SMS específico da mesma versão ou gerar uma nova versão	Gravar	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTemplateActiveVersion	Concede permissão para atualizar o parâmetro de versão ativa de um modelo específico	Gravar	template*		
UpdateVoiceChannel	Concede permissão para atualizar o canal de voz de uma aplicação	Gravar	channel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateVoiceTemplate	Concede permissão para atualizar um modelo de mensagem de voz específico da mesma versão ou gerar uma nova versão	Gravar	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
VerifyOTPMessage	Concede permissão para verificar a validade das senhas de uso único () OTPs	Gravar	verify-otp*		

Tipos de recursos definidos pelo Amazon Pinpoint

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
app	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}`	aws:ResourceTag/${TagKey}
apps	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/*`	

Tipos de recursos	ARN	Chaves de condição
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}
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	

Tipos de recursos	ARN	Chaves de condição
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/${AppId}/messages	
verify-otp	arn:${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}	

Tipos de recursos	ARN	Chaves de condição
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}	
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	

Tipos de recursos	ARN	Chaves de condição
reports	`arn:${Partition}:mobiletargeting:${Region}:${Account}:reports`	

Chaves de condição do Amazon Pinpoint

O Amazon Pinpoint define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por uma chave que está presente na solicitação feita pelo usuário para o serviço Pinpoint	String
aws:ResourceTag/${TagKey}	Filtra o acesso por uma chave da etiqueta e par de valores	String
aws:TagKeys	Filtra o acesso pela lista de todos os nomes de chaves de etiquetas presentes na solicitação feita pelo usuário para o serviço Pinpoint	ArrayOfString

Ações, recursos e chaves de condição do Serviço de e-mail do Amazon Pinpoint

O Serviço de e-mails do Amazon Pinpoint (prefixo do serviço: `ses`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Serviço de e-mail do Amazon Pinpoint
- Tipos de recursos definidos pelo Serviço de e-mail do Amazon Pinpoint
- Chaves de condição do Serviço de e-mail do Amazon Pinpoint

Ações definidas pelo Serviço de e-mail do Amazon Pinpoint

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateConfigurationSet	Concede permissão para criar um conjunto de configurações	Write		ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateConfigurationSetEventDestination	Concede permissão para criar um destino de evento do conjunto de configuração	Write	configuration-set*		
				ses:ApiVersion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
CreateDedicatedIpPool	Concede permissão para criar um novo grupo de endereços IP dedicados	Write		ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateDeliverabilityTestReport	Concede permissão para criar um novo teste de posicionamento de caixa de entrada preditiva	Write	identity*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateEmailIdentity	Concede permissão para iniciar o processo de verificação de uma identidade de e-mail	Write		ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteConfigurationSet	Concede permissão para excluir um conjunto de configurações existente	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteConfigurationSetEventDestination	Concede permissão para excluir um destino de evento	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteDedicatedIpPool	Concede permissão para excluir um grupo de IPs dedicados	Write	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteEmailIdentity	Concede permissão para excluir uma identidade de e-mail que você verificou anteriormente	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetAccount	Concede permissão para obter informações sobre o status e os recursos de envio de e-mail	Read		ses:ApiVersion	
GetBlacklistReports	Concede permissão para recuperar uma lista das listas de negação em que seus endereços IP dedicados aparecem	Read		ses:ApiVersion	
GetConfigurationSet	Concede permissão para obter informações sobre um conjunto de configurações existente	Read	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetConfigurationSetEventDestinations	Concede permissão para recuperar uma lista de destinos de eventos que estão associados a um conjunto de configurações	Read	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDedicatedIp	Concede permissão para obter informações sobre um endereço IP dedicado	Read		ses:ApiVersion	
GetDedicatedIps	Concede permissão para listar os endereços IP dedicados associados à sua conta	Read	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDeliverabilityDashboardOptions	Concede permissão para obter o status do painel de capacidade de entrega	Read		ses:ApiVersion	
GetDeliverabilityTestReport	Concede permissão para recuperar os resultados de um teste de posicionamento de caixa de entrada preditiva	Read	deliverability-test-report*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDomainDeliverabilityCampaign	Concede permissão para recuperar todos os dados de capacidade de entrega de uma campanha específica	Read		ses:ApiVersion	
GetDomainStatisticsReport	Concede permissão para recuperar o posicionamento da caixa de entrada e as taxas de envolvimento dos domínios usados para enviar e-mail	Read	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetEmailIdentity	Concede permissão para obter informações sobre uma identidade específica associada à sua conta	Read	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListConfigurationSets	Concede permissão para listar todos os conjuntos de configurações associados à sua conta	List		ses:ApiVersion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDedicatedIpPools	Concede permissão para listar todos os grupos de IPs dedicados que existem na sua conta	List		ses:ApiVersion	
ListDeliverabilityTestReports	Concede permissão para recuperar uma lista dos testes preditivos de inclusão na caixa de entrada executados, independentemente do status	List		ses:ApiVersion	
ListDomainDeliverabilityCampaigns	Concede permissão para recuperar dados de capacidade e de entrega para todas as campanhas que usaram um domínio específico para enviar e-mails durante um período especificado	Read		ses:ApiVersion	
ListEmailIdentities	Concede permissão para listar todas as identidades de e-mail associadas à sua conta	List		ses:ApiVersion	
ListTagsForResource	Concede permissão para recuperar uma lista de etiquetas (chaves e valores) que estão associados a um recurso específico	Read	configuration-set		
			dedicated-ip-pool		
			deliverability-test-report		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			identity		
				ses:ApiVersion	
PutAccountDedicatedIpWarmupAttributes	Concede permissão para habilitar ou desabilitar o recurso de aquecimento automático para endereços IP dedicados	Write		ses:ApiVersion	
PutAccountSendingAttributes	Concede permissão para ativar ou desativar a capacidade de sua conta de enviar e-mails	Write		ses:ApiVersion	
PutConfigurationSetDeliveryOptions	Concede permissão para associar um conjunto de configurações a um grupo de IPs dedicados	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutConfigurationSetReputationOptions	Concede permissão para habilitar ou desabilitar um conjunto de métricas de reputação para e-mails enviados usando um conjunto de configurações específico	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetSendingOptions	Concede permissão para habilitar ou desabilitar o envio de e-mails para mensagens que usam um conjunto de configurações específico	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetTrackingOptions	Concede permissão para especificar um domínio personalizado a ser usado para elementos de rastreamento de abertura e clique no e-mail que você envia usando um determinado conjunto de configurações	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpInPool	Concede permissão para mover um endereço IP dedicado para um grupo de IPs dedicados existente	Write	dedicated-ip-pool*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpWarmupAttributes	Concede permissão para habilitar atributos de aquecimento de IPs dedicados	Write		ses:ApiVersion	
PutDeliverabilityDashboardOption	Concede permissão para habilitar ou desabilitar o painel de capacidade de entrega	Write		ses:ApiVersion	
PutEmailIdentityDkimAttributes	Concede permissão para habilitar ou desabilitar a autenticação DKIM para uma identidade de e-mail	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityFeedbackAttributes	Concede permissão para habilitar ou desabilitar o encaminhamento de feedback para uma identidade	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutEmailIdentityMailFromAttributes	Concede permissão para habilitar ou desabilitar a configuração do domínio de MAIL FROM personalizado para uma identidade de e-mail	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
SendEmail	Concede permissão para enviar uma mensagem de e-mail	Write	identity*		
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
TagResource	Concede permissão para adicionar uma ou mais etiquetas (chaves e valores) a um recurso especificado	Marcação	configuration-set		
			dedicated-ip-pool		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			deliverability-test-report		
			identity		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover uma ou mais etiquetas (chaves e valores) de um recurso especificado	Marcação	configuration-set		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		
				ses:ApiVersion aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateConfigurationSetEventDestination	Concede permissão para atualizar a configuração de um destino de evento para um conjunto de configurações	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pelo Serviço de e-mail do Amazon Pinpoint

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Tipos de recursos	ARN	Chaves de condição
deliverability-test-report	`arn:${Partition}:ses:${Region}:${Account}:deliverability-test-report/${ReportId}`	aws:ResourceTag/${TagKey}
identity	`arn:${Partition}:ses:${Region}:${Account}:identity/${IdentityName}`	aws:ResourceTag/${TagKey}

Chaves de condição do Serviço de e-mail do Amazon Pinpoint

O Serviço de e-mails do Amazon Pinpoint define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base na presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra ações com base nos pares de chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações com base na presença de chaves da etiqueta na solicitação	ArrayOfString
ses:ApiVersion	Filtra as ações com base na versão da API SES	String
ses:FeedbackAddress	Filtra ações com base no endereço "Return-Path" que especifica para onde as devoluções e reclamações são	String

Chaves de condição	Descrição	Type
	enviadas por encaminhamento de comentários por e-mail.	
ses:FromAddress	Filtra ações com base no endereço “De” de uma mensagem	String
ses:FromDisplayName	Filtra ações com base no endereço “De” que é usado como o nome de exibição de uma mensagem	String
ses:Recipients	Filtra ações com base nos endereços de destinatários de uma mensagem que incluem os endereços "Para", "CC" e "BCC".	ArrayOfString

Ações, recursos e chaves de condição do Serviço de SMS e voz do Amazon Pinpoint

O Serviço de SMS e voz do Amazon Pinpoint (prefixo do serviço: `sms-voice`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Serviço de SMS e voz do Amazon Pinpoint
- Tipos de recursos definidos pelo serviço de SMS e voz do Amazon Pinpoint
- Chaves de condição do serviço de SMS e voz do Amazon Pinpoint

Ações definidas pelo Serviço de SMS e voz do Amazon Pinpoint

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateConfigurationSet	Criar um novo conjunto de configurações. Depois de criar o conjunto de configurações, você pode adicionar um ou mais destinos de eventos a ele.	Write			
CreateConfigurationSetEventDestination	Criar um novo destino de eventos em um conjunto de configurações.	Write			iam:PassRole
DeleteConfigurationSet	Exclui um conjunto de configurações existente.	Write			
DeleteConfigurationSetEventDestination	Exclui um destino de eventos em um conjunto de configurações.	Write			
GetConfigurationSetEventDestinations	Obter informações sobre um destino de eventos, incluindo os tipos de eventos que ele informa, o nome de recurso da Amazon (ARN) do destino e o nome do destino de eventos.	Read			
ListConfigurationSets	Retornar uma lista de conjuntos de configurações. Essa operação retorna apenas os conjuntos de configura	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	ções que estão associados à sua conta na Região da AWS atual.				
SendVoiceMessage	Criar uma nova mensagem de voz e enviá-la para o número de telefone de um destinatário.	Write			
UpdateConfigurationSetEventDestination	Atualizar um destino de eventos em um conjunto de configurações. Um destino de eventos é um local para publicação de informações sobre as suas chamadas de voz. Por exemplo, você pode registrar um evento em um CloudWatch destino da Amazon quando uma chamada falha.	Gravar			iam:PassRole

Tipos de recursos definidos pelo serviço de SMS e voz do Amazon Pinpoint

O Serviço de SMS e voz do Amazon Pinpoint não oferece suporte à especificação do ARN de um recurso no elemento `Resource` de uma instrução de política do IAM. Para conceder acesso ao Serviço de SMS e voz do Amazon Pinpoint, especifique `"Resource": "*"` na política.

Chaves de condição do serviço de SMS e voz do Amazon Pinpoint

O Pinpoint SMS Voice não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do Amazon Polly

O Amazon Polly (prefixo do serviço: `polly`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Polly
- Tipos de recursos definidos pelo Amazon Polly
- Chaves de condição do Amazon Polly

Ações definidas pelo Amazon Polly

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteLexicon	Concede permissão para excluir o léxico de pronúncia especificado armazenado em um Região da AWS	Gravar	lexicon*		
DescribeVoices	Concede permissão para descrever a lista de vozes disponíveis para uso ao solicitar síntese de fala	Lista			
GetLexicon	Concede permissão para recuperar o conteúdo do léxico de pronúncia especific	Leitura	lexicon*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	ado armazenado em um Região da AWS				
GetSpeechSynthesisTask	Concede permissão para obter informações sobre tarefa específica de síntese de fala	Leitura			
ListLexicons	Concede permissão para listar os léxicos de pronúncia armazenados em um Região da AWS	Lista			
ListSpeechSynthesisTasks	Concede permissão para listar tarefas de síntese de fala solicitadas	Lista			
PutLexicon	Concede permissão para armazenar um léxico de pronúncia em um Região da AWS	Gravar	lexicon*		
StartSpeechSynthesisTask	Concede permissão para sintetizar entradas longas para o local fornecido do S3	Gravar	lexicon		s3:PutObject
SynthesizeSpeech	Concede permissão para sintetizar fala	Leitura	lexicon		

Tipos de recursos definidos pelo Amazon Polly

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso

também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
lexicon	`arn:${Partition}:polly:${Region}:${Account}:lexicon/${LexiconName}`	

Chaves de condição do Amazon Polly

O Polly não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Price List

AWS A Lista de preços (prefixo do serviço:`pricing`) fornece os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Price List
- Tipos de recursos definidos pelo AWS Price List
- Chaves de condição do AWS Price List

Ações definidas pelo AWS Price List

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando

usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeServices	Concede permissão para recuperar detalhes do serviço para todos os serviços (paginados, se o serviceCode não estiver definido) ou os detalhes de um serviço específico (se o serviceCode for fornecido)	Leitura			
GetAttributeValues	Concede permissão para recuperar todos os possíveis valores (paginados) para um certo atributo	Leitura			
GetPriceListFileUrl	Concede permissão para recuperar o URL do arquivo da lista de preços para os parâmetros determinados	Leitura			
GetProducts	Concede permissão para recuperar todos os produtos correspondentes com os critérios de pesquisa definidos	Leitura			
ListPriceLists	Concede permissão para listar todas as listas (paginadas) de preços aplicáveis para os parâmetros determinados	Leitura			

Tipos de recursos definidos pelo AWS Price List

AWS A lista de preços não suporta a especificação de um ARN de recurso no elemento de uma `Resource` declaração de política do IAM. Para conceder acesso ao AWS Price List, especifique `"Resource": "*"` na sua política.

Chaves de condição do AWS Price List

O Price List não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o AWS Private CA Connector for Active Directory

AWS O conector CA privado para Active Directory (prefixo do serviço:`pca-connector-ad`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Private CA Connector for Active Directory
- Tipos de recursos definidos pelo AWS Private CA Connector for Active Directory
- Chaves de condição para AWS Private CA Connector for Active Directory

Ações definidas pelo AWS Private CA Connector for Active Directory

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateConnector	Concede permissão para criar um Conector na sua conta	Gravar		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	acm-pca:DescribeCertificateAuthority acm-pca:GetCertificate acm-pca:GetCertificateAuthorityCertificate acm-pca:IssueCertificate ec2:CreateTags ec2:CreateVpcEndpoint ec2:DescribeVpcEndpoints

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDirectoryRegistration	Concede permissão para criar um DirectoryRegistration em sua conta	Gravar		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	ds:AuthorizeApplication ds:DescribeDirectories
CreateServicePrincipalName	Concede permissão para criar um ServicePrincipalName para um DirectoryRegistration	Gravar	DirectoryRegistration*		ds:UpdateAuthorizedApplication
CreateTemplate	Concede permissão para criar um modelo para um conector	Gravar	Connector*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateTemplateGroupAccessControlEntry	Concede permissão para criar um TemplateGroupAccessControlEntry para um modelo	Gravar	Template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteConnector	Concede permissão para excluir um conector na sua conta	Gravar	Connector*		ec2:DeleteVpcEndpoints ec2:DescribeVpcEndpoints
DeleteDirectoryRegistration	Concede permissão para excluir um DirectoryRegistration em sua conta	Gravar	DirectoryRegistration*		ds:UnauthorizeApplication ds:UpdateAuthorizedApplication
DeleteServicePrincipalName	Concede permissão para excluir um ServicePrincipalName para um DirectoryRegistration	Gravar	DirectoryRegistration*		ds:UpdateAuthorizedApplication
DeleteTemplate	Concede permissão para excluir um modelo para um conector	Gravar	Template*		
DeleteTemplateGroupAccessControlEntry	Concede permissão para excluir um TemplateGroupAccessControlEntry para um modelo	Gravar	Template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetConnector	Concede permissão para obter um conector na sua conta	Leitura	Connector*		
GetDirectoryRegistration	Concede permissão para obter um DirectoryRegistration em sua conta	Leitura	DirectoryRegistration*		
GetServicePrincipalName	Concede permissão para obter um ServicePrincipalName para um DirectoryRegistration	Leitura	DirectoryRegistration*		
GetTemplate	Concede permissão para obter um modelo para um conector	Leitura	Template*		
GetTemplateGroupAccessControlEntry	Concede permissão para obter um TemplateGroupAccessControlEntry para um modelo	Leitura	Template*		
ListConnectors	Concede permissão para listar os conectores na sua conta	Lista			
ListDirectoryRegistrations	Concede permissão para listá-los DirectoryRegistrations em sua conta	Lista			
ListServicePrincipalNames	Concede permissão para listar o ServicePrincipalNames para um DirectoryRegistration	Lista	DirectoryRegistration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar as tags de um pca-connector-ad recurso em sua conta	Leitura			
ListTemplateGroupAccessControlEntries	Concede permissão para listar o TemplateGroupAccessControlEntries para um modelo	Lista	Template*		
ListTemplates	Concede permissão para listar os modelos para um conector	Lista	Connector*		
TagResource	Concede permissão para marcar um pca-connector-ad recurso em sua conta	Tags	Connector		
			Directory Registration		
			Template		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um pca-connector-ad recurso em sua conta	Tags	Connector		
			Directory Registration		
			Template		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
UpdateTemplate	Concede permissão para atualizar um modelo para um conector	Gravar	Template*		
UpdateTemplateGroupAccessControlEntry	Concede permissão para atualizar um TemplateGroupAccessControlEntry para um modelo	Gravar	Template*		

Tipos de recursos definidos pelo AWS Private CA Connector for Active Directory

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Tipos de recursos	ARN	Chaves de condição
Template	`arn:${Partition}:pca-connector-ad:${Region}:${Account}:connector/${ConnectorId}/template/${TemplateId}`	aws:ResourceTag/${TagKey}

Chaves de condição para AWS Private CA Connector for Active Directory

AWS O conector CA privado para Active Directory define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Private CA Connector para SCEP

AWS O conector CA privado para SCEP (prefixo de serviço:`pca-connector-scep`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Private CA Connector para SCEP
- Tipos de recursos definidos pelo AWS Private CA Connector para SCEP
- Chaves de condição do AWS Private CA Connector para SCEP

Ações definidas pelo AWS Private CA Connector para SCEP

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateChallenge	Concede permissão para criar um desafio para um conector	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnector	Concede permissão para criar um conector do SCEP na sua conta	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	acm-pca:DescribeCertificateAuthority acm-pca:GetCertificate

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					acm-pca:GetCertificateAuthorityCertificate acm-pca:IssueCertificate
DeleteChallenge	Concede permissão para excluir um desafio para um conector	Gravar	Challenge*		
DeleteConnector	Concede permissão para excluir um conector do SCEP na sua conta	Gravar	Connector*		
GetChallengeMetadata	Concede permissão para obter um desafio para um conector	Leitura	Challenge*		
GetChallengePassword	Concede permissão para obter uma senha de desafio para um conector	Leitura	Challenge*		
GetConnector	Concede permissão para obter um conector do SCEP na sua conta	Leitura	Connector*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListChallengeMetadata	Concede permissão para listar os desafios de um conector	Lista			
ListConnectors	Concede permissão para listar os conectores do SCEP na sua conta	Lista			
ListTagsForResource	Concede permissão para listar as tags de um pca-connector-scep recurso em sua conta	Leitura			
TagResource	Concede permissão para marcar um pca-connector-scep recurso em sua conta	Tags	Challenge		
			Connector		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um pca-connector-scep recurso em sua conta	Tags	Challenge		
			Connector		
				aws:TagKeys	

Tipos de recursos definidos pelo AWS Private CA Connector para SCEP

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações

identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
Challenge	`arn:${Partition}:pca-connector-scep:${Region}:${Account}:connector/${ConnectorId}/challenge/${ChallengeId}`	aws:ResourceTag/${TagKey}
Connector	`arn:${Partition}:pca-connector-scep:${Region}:${Account}:connector/${ConnectorId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Private CA Connector para SCEP

AWS O conector CA privado para SCEP define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento

Chaves de condição	Descrição	Tipo
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para a AWS Private Certificate Authority

AWS A Autoridade de Certificação Privada (prefixo do serviço:`acm-pca`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela AWS Private Certificate Authority
- Tipos de recursos definidos pela AWS Private Certificate Authority
- Chaves de condição para a AWS Private Certificate Authority

Ações definidas pela AWS Private Certificate Authority

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o

nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateCertificateAuthority	Concede permissão para criar uma CA AWS privada e sua	Gravar		aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	chave privada e configuração associadas			aws:ResourceTag/${TagKey} aws:TagKeys	
CreateCertificateAuthorityAuditReport	Concede permissão para criar um relatório de auditoria para uma CA AWS privada	Gravar	certificate-authority*		
CreatePermission	Concede permissão para criar uma permissão para uma CA AWS privada	Gerenciamento de permissões	certificate-authority*		
DeleteCertificateAuthority	Concede permissão para excluir uma CA AWS privada e sua chave privada e configuração associadas	Gravar	certificate-authority*		
DeletePermission	Concede permissão para excluir uma permissão para uma CA AWS privada	Gerenciamento de permissões	certificate-authority*		
DeletePolicy	Concede permissão para excluir a política de uma CA AWS privada	Gerenciamento de permissões	certificate-authority*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeCertificateAuthority	Concede permissão para retornar uma lista dos campos de configuração e status contidos na CA AWS privada especificada	Leitura	certificate-authority*		
DescribeCertificateAuthorityAuditReport	Concede permissão para retornar o status e as informações sobre um relatório de auditoria de CA AWS privada	Leitura	certificate-authority*		
GetCertificate	Concede permissão para recuperar um certificado de CA AWS privada e uma cadeia de certificados para a autoridade de certificação especificada por um ARN	Leitura	certificate-authority*		
GetCertificateAuthorityCertificate	Concede permissão para recuperar um certificado de CA AWS privada e uma cadeia de certificados para a autoridade de certificação especificada por um ARN	Leitura	certificate-authority*		
GetCertificateAuthorityCsr	Concede permissão para recuperar uma solicitação de assinatura de certificado (CSR) de CA AWS privada para a autoridade certificadora especificada por um ARN	Leitura	certificate-authority*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetPolicy	Concede permissão para recuperar a política em uma CA AWS privada	Leitura	certificate-authority*		
ImportCertificateAuthorityCertificate	Concede permissão para importar um SSL/TLS certificado para uma CA AWS privada para uso como o certificado CA de uma CA AWS privada	Gravar	certificate-authority*		
IssueCertificate	Concede permissão para emitir um certificado CA AWS privado	Gravar	certificate-authority*		
				acm-pca:TemplateArn	
ListCertificateAuthorities	Concede permissão para recuperar uma lista da autoridade certificadora ARNs da CA AWS privada e um resumo do status de cada CA na conta de chamada	Lista			
ListPermissions	Concede permissão para listar as permissões que foram aplicadas à autoridade de certificação da CA AWS privada	Leitura	certificate-authority*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTags	Concede permissão para listar as tags que foram aplicadas à autoridade de certificação da CA AWS privada	Leitura	certificate-authority*		
PutPolicy	Concede permissão para colocar uma política em uma CA AWS privada	Gerenciamento de permissões	certificate-authority*		
RestoreCertificateAuthority	Concede permissão para restaurar uma CA AWS privada do estado excluído para o estado em que estava quando foi excluída	Gravar	certificate-authority*		
RevokeCertificate	Concede permissão para revogar um certificado emitido por uma CA AWS privada	Gravar	certificate-authority*		
TagCertificateAuthority	Concede permissão para adicionar uma ou mais tags a uma CA AWS privada	Tags	certificate-authority*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagCertificateAuthority	Concede permissão para remover uma ou mais tags de uma CA AWS privada	Tags	certificate-authority*	aws:RequestTag/${TagKey}	
				aws:TagKeys	
UpdateCertificateAuthority	Concede permissão para atualizar a configuração de uma CA AWS privada	Gravar	certificate-authority*		

Tipos de recursos definidos pela AWS Private Certificate Authority

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
certificate-authority	`arn:${Partition}:acm-pca:${Region}:${Account}:certificate-authority/${CertificateAuthorityId}`	aws:ResourceTag/${TagKey}

Chaves de condição para a AWS Private Certificate Authority

AWS A Autoridade de Certificação Privada define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar

ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
acm-pca:TemplateArn	Filtra o acesso pelo ARN do modelo de certificado usado na solicitação de emissão de certificado	ARN
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS PrivateLink

AWS PrivateLink (prefixo do serviço:`vpce`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS PrivateLink
- Tipos de recursos definidos pelo AWS PrivateLink
- Chaves de condição do AWS PrivateLink

Ações definidas pelo AWS PrivateLink

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AllowMultiRegion [somente permissão]	Concede permissão para gerenciar endpoints de VPC de várias regiões e configurações de serviços de endpoints de VPC	Gravar			

Tipos de recursos definidos pelo AWS PrivateLink

AWS PrivateLink não suporta a especificação de um ARN de recurso no elemento de uma `Resource` declaração de política do IAM. Para conceder acesso ao AWS PrivateLink, especifique `"Resource": "*"` na política.

Chaves de condição do AWS PrivateLink

O VPC Endpoints não tem chaves de contexto específicas do serviço que possam ser usadas no elemento das `Condition` declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Proton

AWS O Proton (prefixo do serviço:`proton`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Proton
- Tipos de recursos definidos pelo AWS Proton
- Chaves de condição do AWS Proton

Ações definidas pelo AWS Proton

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de

recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptEnvironmentAccountConnection	Concede permissão para rejeitar uma solicitação de conexão de conta de ambiente de outra conta de ambiente	Gravar	environment-account-connection*		
CancelComponentDeployment	Concede permissão para cancelar a implantação do componente	Gravar	component*		
CancelEnvironmentDeployment	Concede permissão para cancelar uma implantação de ambiente	Write	environment*		
				proton:EnvironmentTemplate	
CancelServiceInstanceDeployment	Concede permissão para cancelar uma implantação de instância de serviço	Write	service-instance*		
				proton:ServiceTemplate	
CancelServicePipel	Concede permissão para cancelar uma implantação de pipeline de serviço	Gravar	service*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ineDeployment				proton:ServiceTemplate	
CreateComponent	Concede permissão para criar um componente	Gravar	component*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateEnvironment	Concede permissão para criar um ambiente	Write	environment*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey} proton:EnvironmentTemplate	
CreateEnvironmentAccountConnection	Concede permissão para criar uma conexão de conta de ambiente	Write		aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateEnvironmentTemplate	Concede permissão para criar um modelo de ambiente	Gravar	environment-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateEnvironmentTemplateMajorVersion	Concede permissão para criar uma versão principal do modelo de ambiente. OBSOLETO - use em vez disso CreateEnvironmentTemplateVersion	Gravar	environment-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateEnvironmentTemplateMinorVersion	Concede permissão para criar uma versão secundária de modelo de ambiente. OBSOLETO - use em vez disso CreateEnvironmentTemplateVersion	Gravar	environment-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateEnvironmentTemplateVersion	Concede permissão para criar uma versão de modelo de ambiente	Gravar	environment-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateRepository	Concede permissão para criar um repositório	Gravar	repository*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateService	Concede permissão para criar um serviço	Gravar	service*		codestar-connections:PassConnection

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey} proton:ServiceTemplate	
CreateServiceInstance	Concede permissão para criar uma instância de serviço	Gravar	service-instance*		
				aws:TagKeys aws:RequestTag/${TagKey} proton:ServiceTemplate	
CreateServiceSyncConfig	Concede permissão para criar uma configuração de sincronização de serviço	Gravar			
CreateServiceTemplate	Concede permissão para criar um modelo de serviço	Gravar	service-template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateServiceTemplateMajorVersion	Concede permissão para criar uma versão principal do modelo de serviço. OBSOLETO - use em vez disso CreateServiceTemplateVersion	Gravar	service-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateServiceTemplateMinorVersion	Concede permissão para criar uma versão secundária do modelo de serviço. OBSOLETO - use em vez disso CreateServiceTemplateVersion	Gravar	service-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateServiceTemplateVersion	Concede permissão para criar uma versão de modelo de serviço	Gravar	service-template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateTemplateSyncConfig	Concede permissão para criar um modelo sync config	Gravar			
DeleteAccountRoles	Concede permissão para excluir funções da conta. OBSOLETO - use em vez disso UpdateAccountSettings	Gravar			
DeleteComponent	Concede permissão para excluir um componente	Gravar	component*		
DeleteDeployment	Concede permissão para excluir uma implantação	Gravar	deployment*		
DeleteEnvironment	Concede permissão para excluir um ambiente	Write	environment*		
				proton:EnvironmentTemplate	
DeleteEnvironmentAccountConnection	Concede permissão para excluir uma conexão de conta de ambiente	Write	environment-account-connection*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteEnvironmentTemplate	Concede permissão para excluir um modelo de ambiente	Gravar	environment-template*		
DeleteEnvironmentTemplateMajorVersion	Concede permissão para excluir uma versão principal do modelo de ambiente. OBSOLETO - use em vez disso DeleteEnvironmentTemplateVersion	Gravar	environment-template*		
DeleteEnvironmentTemplateMinorVersion	Concede permissão para excluir uma versão secundária do modelo de ambiente. OBSOLETO - use em vez disso DeleteEnvironmentTemplateVersion	Gravar	environment-template*		
DeleteEnvironmentTemplateVersion	Concede permissão para excluir uma versão de modelo de ambiente	Gravar	environment-template*		
DeleteRepository	Concede permissão para excluir um repositório	Gravar	repository*		
DeleteService	Concede permissão para excluir um serviço	Gravar	service*		
				proton:ServiceTemplate	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteServiceSyncConfig	Concede permissão para excluir uma configuração de sincronização de serviço	Gravar			
DeleteServiceTemplate	Concede permissão para excluir um modelo de serviço	Gravar	service-template*		
DeleteServiceTemplateMajorVersion	Concede permissão para excluir uma versão principal do modelo de serviço. OBSOLETO - use em vez disso DeleteServiceTemplateVersion	Gravar	service-template*		
DeleteServiceTemplateMinorVersion	Concede permissão para excluir uma versão secundária do modelo de serviço. OBSOLETO - use em vez disso DeleteServiceTemplateVersion	Gravar	service-template*		
DeleteServiceTemplateVersion	Concede permissão para excluir uma versão de modelo de serviço	Gravar	service-template*		
DeleteTemplateSyncConfig	Concede permissão para excluir um TemplateSyncConfig	Gravar			
GetAccountRoles	Concede permissão para obter funções da conta. OBSOLETO - use em vez disso GetAccountSettings	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAccountSettings	Concede permissão para descrever as configurações da conta	Leitura			
GetComponent	Concede permissão para descrever um componente	Leitura	component*		
GetDeployment	Concede permissão para descrever uma implantação	Leitura	deployment*		
GetEnvironment	Concede permissão para descrever um ambiente	Read	environment*		
GetEnvironmentAccountConnection	Concede permissão para descrever uma conexão de conta de ambiente	Read	environment-account-connection*		
GetEnvironmentTemplate	Concede permissão para descrever um modelo de ambiente	Leitura	environment-template*		
GetEnvironmentTemplateMajorVersion	Concede permissão para obter uma versão principal do modelo de ambiente. OBSOLETO - use em vez disso GetEnvironmentTemplateVersion	Leitura	environment-template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetEnvironmentTemplateMinorVersion	Concede permissão para obter uma versão secundária de modelo de ambiente. OBSOLETO - use em vez disso GetEnvironmentTemplateVersion	Leitura	environment-template*		
GetEnvironmentTemplateVersion	Concede permissão para descrever uma versão de modelo de ambiente	Leitura	environment-template*		
GetRepository	Concede permissão para descrever um repositório	Leitura	repository*		
GetRepositorySyncStatus	Concede permissão para obter o status de sincronização mais recente de um repositório	Leitura			
GetResourceTemplateVersionStatusCounts	Concede permissão para listar contagens de status de versão de modelo de recurso	Leitura			
GetResourcesSummary	Concede permissão para obter um resumo de recursos	Leitura			
GetService	Concede permissão para descrever um serviço	Read	service*		
GetServiceInstance	Concede permissão para descrever uma instância de serviço	Leitura	service-instance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetServiceInstanceSyncStatus	Concede permissão para descrever o status de sincronização de uma instância de serviço	Leitura			
GetServiceSyncBlockerSummary	Concede permissão para descrever bloqueadores de sincronização de serviços de um serviço ou instância de serviço	Leitura			
GetServiceSyncConfig	Concede permissão para descrever uma configuração de sincronização de serviço	Leitura			
GetServiceTemplate	Concede permissão para descrever um modelo de serviço	Leitura	service-template*		
GetServiceTemplateMajorVersion	Concede permissão para obter uma versão principal do modelo de serviço. OBSOLETO - use em vez disso GetServiceTemplateVersion	Leitura	service-template*		
GetServiceTemplateMinorVersion	Concede permissão para obter uma versão secundária do modelo de serviço. OBSOLETO - use em vez disso GetServiceTemplateVersion	Leitura	service-template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetServiceTemplateVersion	Concede permissão para descrever uma versão de modelo de serviço	Leitura	service-template*		
GetTemplateSyncConfig	Concede permissão para descrever um TemplateSyncConfig	Leitura			
GetTemplateSyncStatus	Concede permissão para descrever o status de sincronização de um modelo	Leitura			
ListComponentOutputs	Concede permissão para listar saídas de componente	Lista	component*		
			deployment		
ListComponentProvisionedResources	Concede permissão para listar os recursos provisionados do componente	Lista	component*		
ListComponents	Concede permissão para listar componentes	Lista	environment		
			service		
			service-instance		
ListDeployments	Concede permissão para listar implantações	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListEnvironmentAccountConnections	Concede permissão para listar conexões de conta de ambiente	Lista			
ListEnvironmentOutputs	Concede permissão para listar as saídas do ambiente	Lista	environment*		
			deployment		
ListEnvironmentProvisionedResources	Concede permissão para listar os recursos provisionados do ambiente	Lista	environment*		
ListEnvironmentTemplateMajorVersions	Concede permissão para listar versões principais do modelo de ambiente. OBSOLETO - use em vez disso ListEnvironmentTemplateVersions	Lista	environment-template*		
ListEnvironmentTemplateMinorVersions	Concede permissão para listar versões secundárias de um modelo de ambiente. OBSOLETO - use em vez disso ListEnvironmentTemplateVersions	Lista	environment-template*		
ListEnvironmentTemplateVersions	Concede permissão para listar versões de modelos de ambiente	List	environment-template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListEnvironmentTemplates	Concede permissão para listar modelos de ambiente	List			
ListEnvironments	Concede permissão para listar ambientes	Lista			
ListRepositories	Concede permissão para listar repositórios	Lista			
ListRepositorySyncDefinitions	Concede permissão para listar definições de sincronização do repositório	Lista			
ListServiceInstanceOutputs	Concede permissão para listar as saídas das instâncias de serviço	Lista	service*		
			service-instance*		
			deployment		
ListServiceInstanceProvisionedResources	Concede permissão para listar os recursos provisionados da instância	Lista	service*		
			service-instance*		
ListServiceInstances	Concede permissão para listar instâncias de serviço	Lista			
ListServicePipelineOutputs	Concede permissão para listar as saídas do pipeline de serviço	Lista	service*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			deployment		
ListServicePipelineProvisionedResources	Concede permissão para listar os recursos provisionados do pipeline	Lista	service*		
ListServiceTemplateMajorVersions	Concede permissão para listar as principais versões do modelo de serviço. OBSOLETO - use em vez disso ListServiceTemplateVersions	Lista	service-template*		
ListServiceTemplateMinorVersions	Concede permissão para listar versões secundárias do modelo de serviço. OBSOLETO - use em vez disso ListServiceTemplateVersions	Lista	service-template*		
ListServiceTemplateVersions	Concede permissão para listar versões de modelos de serviço	List	service-template*		
ListServiceTemplates	Concede permissão para listar modelos de serviço	List			
ListServices	Concede permissão para listar serviços	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar etiquetas de um recurso	Leitura	component		
			environment		
			environment-account-connection		
			environment-template		
			environment-template-major-version		
			environment-template-minor-version		
			environment-template-version		
			repository		
			service		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			service-instance		
			service-template		
			service-template-major-version		
			service-template-minor-version		
			service-template-version		
NotifyResourceDeploymentStatusChange	Concede permissão para notificar o Proton sobre alterações de status de implantação de recursos	Gravar	environment		
			service-instance		
RejectEnvironmentAccountConnection	Concede permissão para rejeitar uma solicitação de conexão de conta de ambiente de outra conta de ambiente	Gravar	environment-account-connection*		
TagResource	Concede permissão para adicionar tags a um recurso	Marcação	component		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			environment		
			environment-account-connection		
			environment-template		
			environment-template-major-version		
			environment-template-minor-version		
			environment-template-version		
			repository		
			service		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			service-instance		
			service-template		
			service-template-major-version		
			service-template-minor-version		
			service-template-version		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover etiquetas de um recurso	Tags	component		
			environment		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			environment-account-connection		
			environment-template		
			environment-template-major-version		
			environment-template-minor-version		
			environment-template-version		
			repository		
			service		
			service-instance		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			service-template		
			service-template-major-version		
			service-template-minor-version		
			service-template-version		
				aws:TagKeys	
UpdateAccountRoles	Concede permissão para atualizar as funções da conta. OBSOLETO - use em vez disso UpdateAccountSettings	Gravar			iam:PassRole
UpdateAccountSettings	Concede permissão para atualizar as configurações da conta	Gravar			iam:PassRole
UpdateComponent	Concede permissão para atualizar um componente	Gravar	component*		
UpdateEnvironment	Concede permissão para atualizar um ambiente	Write	environment*		iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				proton:EnvironmentTemplate	
UpdateEnvironmentAccountConnection	Concede permissão para atualizar uma conexão de conta de ambiente	Write	environment-account-connection*		
UpdateEnvironmentTemplate	Concede permissão para atualizar um modelo de ambiente	Gravar	environment-template*		
UpdateEnvironmentTemplateMajorVersion	Concede permissão para atualizar uma versão principal do modelo de ambiente. OBSOLETO - use em vez disso UpdateEnvironmentTemplateVersion	Gravar	environment-template*		
UpdateEnvironmentTemplateMinorVersion	Concede permissão para atualizar uma versão secundária do modelo de ambiente. OBSOLETO - use em vez disso UpdateEnvironmentTemplateVersion	Gravar	environment-template*		
UpdateEnvironmentTemplateVersion	Concede permissão para atualizar uma versão de modelo de ambiente	Write	environment-template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateService	Concede permissão para atualizar um serviço	Write	service*		
				proton:ServiceTemplate	
UpdateServiceInstance	Concede permissão para atualizar uma instância de serviço	Write	service-instance*		
				proton:ServiceTemplate	
UpdateServicePipeline	Concede permissão para atualizar um pipeline de serviço	Gravar	service*		
				proton:ServiceTemplate	
UpdateServiceSyncBlocker	Concede permissão para atualizar um bloqueador de sincronização de serviço	Gravar			
UpdateServiceSyncConfig	Concede permissão para atualizar uma configuração de sincronização de serviço	Gravar			
UpdateServiceTemplate	Concede permissão para atualizar um modelo de serviço	Gravar	service-template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateServiceTemplateMajorVersion	Concede permissão para atualizar uma versão principal do modelo de serviço. OBSOLETO - use em vez disso UpdateServiceTemplateVersion	Gravar	service-template*		
UpdateServiceTemplateMinorVersion	Concede permissão para criar uma versão secundária do modelo de serviço. OBSOLETO - use em vez disso UpdateServiceTemplateVersion	Gravar	service-template*		
UpdateServiceTemplateVersion	Concede permissão para atualizar uma versão de modelo de serviço	Gravar	service-template*		
UpdateTemplateSyncConfig	Concede permissão para atualizar um TemplateSyncConfig	Gravar			

Tipos de recursos definidos pelo AWS Proton

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
environment-template	arn:${Partition}:proton:${Region}:${Account}:environment-template/${Name}	aws:ResourceTag/${TagKey}
environment-template-version	arn:${Partition}:proton:${Region}:${Account}:environment-template/${TemplateName}:${MajorVersion}.${MinorVersion}	aws:ResourceTag/${TagKey}
environment-template-major-version	arn:${Partition}:proton:${Region}:${Account}:environment-template/${TemplateName}:${MajorVersionId}	aws:ResourceTag/${TagKey}
environment-template-minor-version	arn:${Partition}:proton:${Region}:${Account}:environment-template/${TemplateName}:${MajorVersionId}.${MinorVersionId}	aws:ResourceTag/${TagKey}
service-template	arn:${Partition}:proton:${Region}:${Account}:service-template/${Name}	aws:ResourceTag/${TagKey}
service-template-version	arn:${Partition}:proton:${Region}:${Account}:service-template/${TemplateName}:${MajorVersion}.${MinorVersion}	aws:ResourceTag/${TagKey}
service-template-major-version	arn:${Partition}:proton:${Region}:${Account}:service-template/${TemplateName}:${MajorVersionId}	aws:ResourceTag/${TagKey}
service-template-minor-version	arn:${Partition}:proton:${Region}:${Account}:service-template/${TemplateName}:${MajorVersionId}.${MinorVersionId}	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
environment	`arn:${Partition}:proton:${Region}:${Account}:environment/${Name}`	aws:ResourceTag/${TagKey}
service	`arn:${Partition}:proton:${Region}:${Account}:service/${Name}`	aws:ResourceTag/${TagKey}
service-instance	`arn:${Partition}:proton:${Region}:${Account}:service/${ServiceName}/service-instance/${Name}`	aws:ResourceTag/${TagKey}
environment-account-connection	`arn:${Partition}:proton:${Region}:${Account}:environment-account-connection/${Id}`	aws:ResourceTag/${TagKey}
repository	`arn:${Partition}:proton:${Region}:${Account}:repository/${Provider}:${Name}`	aws:ResourceTag/${TagKey}
component	`arn:${Partition}:proton:${Region}:${Account}:component/${Id}`	aws:ResourceTag/${TagKey}
deployment	`arn:${Partition}:proton:${Region}:${Account}:deployment/${Id}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Proton

AWS O Proton define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta na solicitação	ArrayOfString
proton:EnvironmentTemplate	Filtra o acesso por um modelo de ambiente especificado relacionado a um recurso	String
proton:ServiceTemplate	Filtra o acesso por um modelo de serviço especificado relacionado a um recurso	String

Ações, recursos e chaves de condição do console do AWS Purchase Orders

AWS O Purchase Orders Console (prefixo do serviço:`purchase-orders`) fornece os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo console do AWS Purchase Orders
- Tipos de recursos definidos pelo console do AWS Purchase Orders
- Chaves de condição do console do AWS Purchase Orders

Ações definidas pelo console do AWS Purchase Orders

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddPurchaseOrder [somente permissão]	Concede permissão para adicionar uma nova ordem de compra	Gravar	purchase-order*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeletePurchaseOrder [somente permissão]	Concede permissão para excluir uma ordem de compra	Gravar	purchase-order*		
				aws:ResourceTag/${TagKey}	
GetConsoleActionSetEnforced [somente permissão]	Concede permissão para visualizar se ações do IAM existentes ou refinadas estão sendo usadas para controlar a autorização para os consoles de Faturamento, Gerenciamento de Custos e Contas	Leitura			
GetPurchaseOrder [somente permissão]	Concede permissão para obter uma ordem de compra	Leitura	purchase-order*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListPurchaseOrderInvoices [somente permissão]	Concede permissão para listar faturas de ordem de compra	Lista	purchase-order*		
				aws:ResourceTag/${TagKey}	
ListPurchaseOrders [somente permissão]	Concede permissão para listar todas as ordens de compra de uma conta	Lista			
ListTagsForResource [somente permissão]	Concede permissão para listar tags de uma ordem de compra	Leitura	purchase-order		
				aws:ResourceTag/${TagKey}	
ModifyPurchaseOrders [somente permissão]	Concede permissão para modificar detalhes e ordens de compra	Gravar	purchase-order*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource [somente permissão]	Concede permissão para marcar ordens de compra com pares de chave-valor fornecidos	Tags	purchase-order*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource [somente permissão]	Concede permissão para remover tags de uma ordem de compra	Tags	purchase-order*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateConsoleActionSetEnforced [somente permissão]	Concede permissão para alterar se ações do IAM existentes ou refinadas serão usadas para controlar a autorização para os consoles de Faturamento, Gerenciamento de Custos e Contas	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdatePurchaseOrder [somente permissão]	Concede permissão para atualizar uma ordem de compra existente	Gravar	purchase-order*		
				aws:ResourceTag/${TagKey}	
UpdatePurchaseOrderStatus [somente permissão]	Concede permissão para definir status da ordem de compra	Gravar	purchase-order*		
				aws:ResourceTag/${TagKey}	
ViewPurchaseOrders [somente permissão]	Concede permissão para visualizar detalhes e ordens de compra	Leitura	purchase-order		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pelo console do AWS Purchase Orders

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
purchase-order	`arn:${Partition}:purchase-orders::${Account}:purchase-order/${ResourceName}`	aws:ResourceTag/${TagKey}

Chaves de condição do console do AWS Purchase Orders

AWS O console de pedidos de compra define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso pela chave e valor de uma etiqueta em uma solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelo conjunto de pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta em uma solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Q

O Amazon Q (prefixo do serviço: q) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Q
- Tipos de recursos definidos pelo Amazon Q
- Chaves de condição do Amazon Q

Ações definidas pelo Amazon Q

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de

condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateConnectorResource [somente permissão]	Concede permissão para associar um AWS recurso a um conector Amazon Q	Gravar			
CreateAssignment [somente permissão]	Concede permissão para criar uma atribuição de usuário ou grupo de um perfil do Amazon Q Developer	Gravar	profile*		
				identitystore:UserId identitystore:GroupId	
CreateAuthGrant	Concede permissão para criar OAuth usuário no Amazon Q	Gravar			kms:Decrypt

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
[somente permissão]					kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
CreateOAuthAppConnection [somente permissão]	Concede permissão para registrar um OAuth aplicativo no Amazon Q	Gravar			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
CreatePlugin [somente permissão]	Concede permissão para criar e configurar um plug-in de terceiros no Amazon Q	Gravar	plugin*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteAssignment [somente permissão]	Concede permissão para excluir uma atribuição de usuário ou grupo de um perfil do Amazon Q Developer	Gravar	profile*		
				identitystore:UserId identitystore:GroupId	
DeleteConversation [somente permissão]	Concede permissão para excluir uma conversa com a Amazon Q	Gravar			
DeleteOAuthAppConnection [somente permissão]	Concede permissão para excluir um OAuth aplicativo no Amazon Q	Gravar			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
DeletePlugin [somente permissão]	Concede permissão para excluir um plug-in configurado no Amazon Q	Gravar	plugin*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GenerateCodeFromCommands [somente permissão]	Concede permissão para gerar código usando comandos da CLI no Amazon Q	Leitura			
GenerateCodeRecommendations [somente permissão]	Concede permissão para gerar recomendações de código no Amazon Q	Leitura			
GetConnector [somente permissão]	Concede permissão para visualizar informações sobre um conector Amazon Q específico	Leitura			
GetConversation [somente permissão]	Concede permissão para obter mensagens individuais associadas a uma conversa específica com o Amazon Q	Leitura			
GetIdentityMetadata [somente permissão]	Concede permissão ao Amazon Q para obter os metadados de identidade	Leitura			
GetPlugin [somente permissão]	Concede permissão para visualizar informações sobre um plug-in Amazon Q configurado específico	Leitura	plugin*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetTroubleshootingResults [somente permissão]	Concede permissão para obter resultados de solução de problemas com o Amazon Q	Leitura			
ListConversations [somente permissão]	Concede permissão para listar conversas individuais associadas a um usuário específico do Amazon Q	Leitura			
ListDashboardMetrics [somente permissão]	Concede permissão para ler métricas para preencher o painel do Amazon Q	Lista			
ListPluginProviders [somente permissão]	Concede permissão para listar plug-ins disponíveis no Amazon Q	Lista			
ListPlugins [somente permissão]	Concede permissão para listar plug-ins configurados no Amazon Q	Lista	plugin*		
ListTagsForResource [somente permissão]	Concede permissão para listar todas as tags associadas a um recurso do Amazon Q	Lista	plugin		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PassRequest [somente permissão]	Concede permissão para permitir que o Amazon Q execute ações em seu nome	Gravar			
RejectConnector [somente permissão]	Concede permissão para rejeitar uma solicitação de conexão para um conector Amazon Q	Gravar			
SendEvent [somente permissão]	Concede permissão para acionar ações assíncronas do Amazon Q	Gravar			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
SendMessage [somente permissão]	Concede permissão para enviar uma mensagem para a Amazon Q	Gravar			
StartConversation [somente permissão]	Concede permissão para iniciar uma conversa com a Amazon Q	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartTroubleshootingAnalysis [somente permissão]	Concede permissão para iniciar uma análise de solução de problemas com o Amazon Q	Gravar			
StartTroubleshootingResolutionExplanation [somente permissão]	Concede permissão para iniciar uma explicação de solução de problemas com o Amazon Q	Gravar			
TagResource [somente permissão]	Concede permissão para associar tags a um recurso do Amazon Q	Tags	plugin		
				aws:ResourceTag/${TagKey} aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [somente permissão]	Concede permissão para remover tags associadas a um recurso do Amazon Q	Tags	plugin		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateAuthGrant [somente permissão]	Concede permissão para atualizar OAuth o usuário no Amazon Q	Gravar			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
UpdateConversation [somente permissão]	Concede permissão para atualizar uma conversa com a Amazon Q	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateOAuthAppConnection [somente permissão]	Concede permissão para atualizar um OAuth aplicativo no Amazon Q	Gravar			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
UpdatePlugin [somente permissão]	Concede permissão para atualizar um plug-in de terceiros no Amazon Q	Gravar	plugin*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateTroubleshootingCommandResult [somente permissão]	Concede permissão para atualizar um resultado de comando de solução de problemas com o Amazon Q	Gravar			
UsePlugin [somente permissão]	Concede permissão para usar os plug-ins do Amazon Q	Gravar	plugin*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
VerifyOAuthAppConnection [somente permissão]	Concede permissão para verificar um OAuth aplicativo no Amazon Q	Gravar			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo

Tipos de recursos definidos pelo Amazon Q

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
profile	`arn:${Partition}:codewhisperer:${Region}:${Account}:profile/${Identifier}`	
plugin	`arn:${Partition}:qdeveloper:${Region}:${Account}:plugin/${Identifier}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Q

O Amazon Q define as chaves de condição a seguir que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas tags associadas ao recurso Amazon Q	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString
identitystore:GroupId	Filtra o acesso por ID de grupo do Centro de Identidade do IAM	ArrayOfString
identitystore:UserId	Filtra o acesso pelo ID de usuário do IAM Identity Center	ArrayOfString

Ações, recursos e chaves de condição do Amazon Q Business

O Amazon Q Business (prefixo do serviço: `qbusiness`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.

- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Q Business
- Tipos de recursos definidos pelo Amazon Q Business
- Chaves de condição do Amazon Q Business

Ações definidas pelo Amazon Q Business

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AllowVendedLogDeliveryForResource [somente permissão]	Concede permissão para configurar a entrega de logs fornecidos para o recurso de aplicação do Amazon Q Business	Gerenciamento de permissões	application*		
				aws:ResourceTag/${TagKey}	
AssociatePermission	Concede permissão para associar uma declaração de política baseada em recursos ao aplicativo	Gravar	application*		qbusiness:PutResourcePolicy
BatchDeleteDocument	Concede permissão para excluir documentos em lote	Gravar	application*		
			index*		
BatchPutDocument	Conceder permissão para colocar documento em lote	Gravar	application*		
			index*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelSubscription	Concede permissão para cancelar uma assinatura	Gravar	application*		
			subscription*		
Chat	Concede permissão para conversar usando uma aplicação	Leitura	application*		
ChatSync	Concede permissão para conversar de forma síncrona usando uma aplicação	Leitura	application*		
CheckDocumentAccess	Concede permissão para verificar se um usuário tem acesso a um documento	Leitura	application*		
			index*		
CreateAnonymousWebExperienceUrl	Concede permissão para criar uma URL exclusiva para uma experiência anônima na web do Amazon Q Business	Gravar	application*		
			web-experience*		
CreateApplication	Concede permissão para criar um aplicativo	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateChatResponseConfiguration	Concede permissão para criar uma configuração de resposta de bate-papo para o aplicativo	Gravar	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataAccessor	Concede permissão para DataAccessor criar no aplicativo	Gravar	application*		qbusiness:CreateDataAccessorWithTti
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataAccessorWithTti [somente permissão]	Concede permissão para criar o AWS IAM Identity Center Trusted Token Issuer com base DataAccessor no aplicativo	Gravar	application*		
CreateDataSource	Concede permissão para criar uma fonte de dados para determinada aplicação e índice	Gravar	application*		
			index*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIndex	Concede permissão para criar um índice para determinada aplicação	Gravar	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIntegration	Concede permissão para criar uma nova integração para um aplicativo Q Business	Gravar	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePlugin	Concede permissão para criar um plug-in para determinada aplicação	Gravar	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRetriever	Concede permissão para criar um recuperador para determinada aplicação	Gravar	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscription	Concede permissão para criar uma assinatura	Gravar	application*		
				identitystore:UserId identitystore:GroupId	
CreateUser	Concede permissão para criar um usuário	Gravar	application*		
CreateWebExperience	Concede permissão para criar uma experiência da Web para determinada aplicação	Gravar	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Concede permissão para excluir um aplicativo	Gravar	application*		
DeleteAttachment	Concede permissão para excluir um anexo no contexto atual do bate-papo	Gravar	application*		
DeleteChatControlsConfiguration	Concede permissão para excluir uma configuração de controle de chat para uma aplicação	Gravar	application*		
DeleteChatResponseConfiguration	Concede permissão para excluir uma configuração de resposta de bate-papo	Gravar	application*		
			chat-response-configuration*		
DeleteConversation	Concede permissão para excluir uma conversa	Gravar	application*		
DeleteDataAccessor	Concede permissão para excluir DataAccessor	Gravar	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			data-accessor*		
DeleteDataSource	Concede permissão para excluir um DataSource	Gravar	application*		
			data-source*		
			index*		
DeleteGroup	Concede permissão para excluir um grupo	Gravar	application*		
			index*		
DeleteIndex	Concede permissão para excluir um índice	Gravar	application*		
			index*		
DeleteIntegration	Concede permissão para excluir uma integração para um aplicativo Q Business	Gravar	application*		
			integration*		
DeletePlugin	Concede permissão para excluir um plug-in	Gravar	application*		
			plugin*		
DeleteRetriever	Concede permissão para excluir um recuperador	Gravar	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			retriever*		
DeleteUser	Concede permissão para excluir um usuário	Gravar	application*		
DeleteWebExperience	Concede permissão para excluir uma experiência da Web	Gravar	application*		
			web-experience*		
DisableAclOnDataSource [somente permissão]	Concede permissão para desabilitar o crawling de ACL ao criar o recurso de fonte de dados do Amazon Q Business	Gravar	application*		
DisassociatePermission	Concede permissão para desassociar a declaração de política baseada em recursos ao aplicativo	Gravar	application*		qbusiness:PutResourcePolicy
GetApplication	Concede permissão para obter uma aplicação	Leitura	application*		
GetChatControlsConfiguration	Concede permissão para obter uma configuração de controle de chat para uma aplicação	Lista	application*		
GetChatResponseConfiguration	Concede permissão para obter uma configuração de resposta de chat	Leitura	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			chat-response-configuration*		
GetDataAccessor	Concede permissão para obter DataAccessor	Leitura	application*		
			data-accessor*		
GetDataSource	Concede permissão para obter uma fonte de dados	Leitura	application*		
			data-source*		
			index*		
GetDocumentContent	Concede permissão para obter o conteúdo de um documento	Leitura	application*		
			index*		
GetGroup	Concede permissão para obter um grupo	Leitura	application*		
			index*		
GetIndex	Concede permissão para obter um índice	Leitura	application*		
			index*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetIntegration	Concede permissão para obter uma integração para um aplicativo Q Business	Leitura	application*		
			integration*		
GetMedia	Concede permissão para obter a mídia associada a uma mensagem do sistema	Leitura	application*		
GetPlugin	Concede permissão para obter um plug-in	Leitura	application*		
			plugin*		
GetPolicy	Concede permissão para obter a política baseada em recursos do aplicativo	Leitura	application*		
GetRetriever	Concede permissão para obter um recuperador	Leitura	application*		
			retriever*		
GetUser	Concede permissão para obter um usuário	Leitura	application*		
GetWebExperience	Concede permissão para obter uma experiência da Web	Leitura	application*		
			web-experience*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListApplications	Concede permissão para listar as aplicações	Lista			
ListAttachments	Concede permissão para listar anexos no contexto atual do bate-papo	Lista	application*		
ListChatResponseConfigurations	Concede permissão para listar as configurações de resposta de bate-papo para um aplicativo	Lista	application*		
ListConversations	Concede permissão para listar todas as conversas para uma aplicação	Lista	application*		
ListDataAccessors	Concede permissão para listar DataAccessors para o aplicativo	Lista	application*		
ListDataSourceSyncJobs	Concede permissão para obter histórico de trabalho de sincronização de origem dos dados	Lista	application*		
			data-source*		
			index*		
ListDataSources	Concede permissão para listar as fontes de dados de uma aplicação e de um índice	Lista	application*		
			index*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDocuments	Concede permissão para listar todos os documentos	Lista	application*		
			index*		
ListGroups	Concede permissão para listar grupos	Lista	application*		
			index*		
ListIndices	Concede permissão para listar os índices de uma aplicação	Lista	application*		
ListIntegrations	Concede permissão para listar todas as integrações de um aplicativo Q Business	Lista	application*		
ListMessages	Concede permissão para listar todas as mensagens	Lista	application*		
ListPluginActions	Concede permissão para listar as ações de plug-ins de um plug-in dentro do aplicativo	Leitura	application*		
			plugin*		
ListPluginTypeActions	Concede permissão para listar todas as ações de um tipo de plug-in	Leitura			
ListPluginTypeMetadata	Concede permissão para listar todos os metadados do tipo de plug-in	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListPlugins	Concede permissão para listar os plugins de uma aplicação	Lista	application*		
ListRetrievers	Concede permissão para listar os recuperadores de uma aplicação	Lista	application*		
ListSubscriptions	Concede permissão para listar assinaturas	Lista	application*		
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	application		
			chat-response-configuration		
			data-accessor		
			data-source		
			index		
			integration		
			plugin		
			retriever		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			web-experience		
ListWebExperiences	Concede permissão para listar as experiências da Web de uma aplicação	Lista	application*		
PutFeedback	Concede permissão para adicionar comentários sobre uma mensagem de conversa	Gravar	application*		
PutGroup	Concede permissão para adicionar um grupo de usuários	Gravar	application*		
			index*		
PutResourcePolicy [somente permissão]	Concede permissão para colocar uma declaração de política baseada em recursos no aplicativo	Gravar	application*		
SearchRelevantContent	Concede permissão para pesquisar conteúdo relevante no aplicativo Amazon Q Business	Leitura	application*		
StartDataSourceSyncJob	Concede permissão para iniciar o trabalho de sincronização de origem dos dados	Gravar	application*		
			data-source*		
			index*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartDeployment	Concede permissão para iniciar a implantação de uma integração	Gravar	application*		
			integration*		
StopDataSourceSyncJob	Concede permissão para interromper o trabalho de sincronização de origem dos dados	Gravar	application*		
			data-source*		
			index*		
TagResource	Concede permissão para marcar um recurso com determinados pares de chave-valor	Tags	application		
			chat-response-configuration		
			data-accessor		
			data-source		
			index		
			integration		
			plugin		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			retriever		
			web-experience		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover a etiqueta com a chave fornecida de um recurso	Tags	application		
			chat-response-configuration		
			data-accessor		
			data-source		
			index		
			integration		
			plugin		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			retriever		
			web-experience		
				aws:TagKeys	
UpdateApplication	Concede permissão para atualizar uma aplicação	Gravar	application*		
UpdateChatControlsConfiguration	Concede permissão para atualizar uma configuração de controle de chat para uma aplicação	Gravar	application*		
UpdateChatResponseConfiguration	Concede permissão para atualizar uma configuração de resposta de chat	Gravar	application*		
			chat-response-configuration*		
UpdateDataAccessor	Concede permissão para atualizar DataAccessor	Gravar	application*		
			data-accessor*		
UpdateDataSource	Concede permissão para atualizar um DataSource	Gravar	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			data-source*		
			index*		
UpdateIndex	Concede permissão para atualizar um índice	Gravar	application*		
			index*		
UpdateIntegration	Concede permissão para atualizar uma integração para um aplicativo Q Business	Gravar	application*		
			integration*		
UpdatePlugin	Concede permissão para atualizar um plug-in	Gravar	application*		
			plugin*		
UpdateRetriever	Concede permissão para atualizar um recuperador	Gravar	application*		
			retriever*		
UpdateSubscription	Concede permissão para atualizar uma assinatura	Gravar	application*		
			subscription*		
UpdateUser	Concede permissão para atualizar um usuário	Gravar	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateWebExperience	Concede permissão para atualizar um WebExperience	Gravar	application*		
			web-experience*		

Tipos de recursos definidos pelo Amazon Q Business

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
application	`arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}`	aws:ResourceTag/${TagKey}
integration	`arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/integration/${IntegrationId}`	aws:ResourceTag/${TagKey}
retriever	`arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/retriever/${RetrieverId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
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/${TagKey}
subscription	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/subscription/${SubscriptionId}	
data-accessor	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/data-accessor/${DataAccessorId}	aws:ResourceTag/${TagKey}
chat-response-configuration	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/chat-response-configuration/${ChatResponseConfigurationId}	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Q Business

O Amazon Q Business define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as

condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString
identitystore:GroupId	Filtra o acesso por ID de grupo do Centro de Identidade do IAM	ArrayOfString
identitystore:UserId	Filtra o acesso pelo ID de usuário do IAM Identity Center	ArrayOfString

Ações, recursos e chaves de condição para aplicações do Q do Amazon Q Business

As aplicações do Q do Amazon Q Business (prefixo do serviço: `qapps`) fornecem os recursos, ações e chaves de contexto de condição a seguir específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelas aplicações do Q do Amazon Q Business
- Tipos de recursos definidos por aplicações do Q do Amazon Q Business
- Chaves de condição de aplicações do Q do Amazon Q Business

Ações definidas pelas aplicações do Q do Amazon Q Business

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateLibraryItemReview	Concede permissão para associar uma revisão de item de biblioteca no ambiente de aplicações do Q Business	Gravar	qapp*		
				qapps:UserIsAppOwner qapps:AppIsPublished	
AssociateQAppWithUser	Concede permissão para associar a aplicação do Q a um usuário no ambiente de aplicações do Q Business	Gravar	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchCreateCategory	Concede permissão para criar as categorias de uma biblioteca no ambiente de aplicativos Q Business	Gravar	application*		
BatchDeleteCategory	Concede permissão para excluir as categorias de uma biblioteca no ambiente do aplicativo Q Business	Gravar	application*		
BatchUpdateCategory	Concede permissão para atualizar as categorias de uma biblioteca no ambiente de aplicativos Q Business	Gravar	application*		
CopyQApp [somente permissão]	Concede permissão para copiar a aplicação do Q no ambiente de aplicações do Q Business	Gravar	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
CreateLibraryItem	Concede permissão para criar um item de biblioteca no ambiente de aplicações do Q Business	Gravar	application		
			qapp		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				qapps:UserIsAppOwner qapps:AppIsPublished	
CreateLibraryItemReview [somente permissão]	Concede permissão para criar uma revisão de item de biblioteca no ambiente de aplicações do Q Business	Gravar	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
CreateQApp	Concede permissão para criar uma aplicação do Q no ambiente de aplicações do Q Business	Gravar	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSubscriptionToken [somente permissão]	Concede permissão para assinar um tópico do barramento de eventos da aplicação do Q no ambiente de aplicações do Q Business	Gravar	application*		
DeleteLibraryItem	Concede permissão para excluir um item de biblioteca no ambiente de aplicações do Q Business	Gravar	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
DeleteQApp	Concede permissão para excluir a aplicação do Q no ambiente de aplicações do Q Business	Gravar	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeQAppPermissions	Concede permissão para obter permissões de compartilhamento do Q App no ambiente do aplicativo Q Business	Leitura	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
DisassociateLibraryItemReview	Concede permissão para desassociar uma revisão de item de biblioteca no ambiente de aplicações do Q Business	Gravar	qapp*		
				qapps:UserIsAppOwner qapps:AppIsPublished	
DisassociateQAppFromUser	Concede permissão para desassociar a aplicação do Q de um usuário no ambiente de aplicações do Q Business	Gravar	application		
			qapp		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				qapps:UserIsAppOwner qapps:AppIsPublished	
ExportQAppSessionData	Concede permissão para exportar dados da sessão da aplicação do Q no ambiente de aplicações do Q Business	Gravar	qapp-session*		
GetLibraryItem	Concede permissão para obter um item de biblioteca no ambiente de aplicações do Q Business	Leitura	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
GetQApp	Concede permissão para obter a aplicação do Q no ambiente de aplicações do Q Business	Leitura	application		
			qapp		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				qapps:UserIsAppOwner qapps:AppIsPublished	
GetQAppSession	Concede permissão para obter uma sessão da aplicação do Q no ambiente de aplicações do Q Business	Leitura	qapp-session*		
				qapps:UserIsAppOwner qapps:AppIsPublished qapps:UserIsSessionModerator qapps:SessionIsShared	
GetQAppSessionMetadata	Concede permissão para obter metadados da sessão da aplicação do Q no ambiente de aplicações do Q Business	Leitura	qapp-session*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ImportDocument	Concede permissão para importar um documento para a aplicação do Q ou a sessão de aplicação do Q no ambiente de aplicações do Q Business	Gravar	qapp		
			qapp-session		
				qapps:UserIsAppOwner qapps:AppIsPublished qapps:UserIsSessionModerator qapps:SessionIsShared	
ListCategories	Concede permissão para listar categorias no ambiente de aplicativos Q Business	Lista	application*		
ListLibraryItems	Concede permissão para listar itens de biblioteca no ambiente de aplicações do Q Business	Lista	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListQAppSessionData	Concede permissão para obter dados da sessão da aplicação do Q no ambiente de aplicações do Q Business	Leitura	qapp-session*		
ListQApps	Concede permissão para listar aplicações do Q no ambiente de aplicações do Q Business	Lista	application*		
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	qapp		
			qapp-session		
PredictProblemStatementFromConversation [somente permissão]	Concede permissão para prever a declaração do problema usando o log de conversas no ambiente de aplicações do Q Business	Gravar	application*		
PredictQApp	Concede permissão para prever a aplicação do Q usando o log de conversas ou a declaração do problema no ambiente de aplicações do Q Business	Gravar	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PredictQAppFromProblemStatement [somente permissão]	Concede permissão para prever os metadados da aplicação do Q usando a declaração do problema no ambiente de aplicações do Q Business	Gravar	application*		
StartQAppSession	Concede permissão para iniciar uma sessão da aplicação do Q no ambiente de aplicações do Q Business	Gravar	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished aws:RequestTag/${TagKey} aws:TagKeys	
StopQAppSession	Concede permissão para interromper a sessão da aplicação do Q no ambiente de aplicações do Q Business	Gravar	application		
			qapp-session		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				qapps:UserIsAppOwner qapps:AppIsPublished qapps:UserIsSessionModerator qapps:SessionIsShared	
TagResource	Concede permissão para marcar um recurso com determinados pares de chave-valor	Tags	qapp		
			qapp-session		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover a etiqueta com a chave fornecida de um recurso	Tags	qapp		
			qapp-session		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
UpdateLibraryItem	Concede permissão para atualizar um item de biblioteca no ambiente de aplicações do Q Business	Gravar	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
UpdateLibraryItemMetadata	Concede permissão para atualizar os metadados de um item de biblioteca no ambiente de aplicações do Q Business	Gravar	qapp*		
				qapps:AppIsPublished	
UpdateQApp	Concede permissão para atualizar a aplicação do Q no ambiente de aplicações do Q Business	Gravar	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateQAppPermissions	Concede permissão para atualizar as permissões de compartilhamento do Q App no ambiente do aplicativo Q Business	Gravar	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
UpdateQAppSession	Concede permissão para atualizar a sessão da aplicação do Q no ambiente de aplicações do Q Business	Gravar	qapp-session*		
				qapps:UserIsAppOwner qapps:AppIsPublished qapps:UserIsSessionModerator qapps:SessionIsShared	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateQAppSessionMetadata	Concede permissão para atualizar os metadados da sessão da aplicação do Q no ambiente de aplicações do Q Business	Gravar	qapp-session*		

Tipos de recursos definidos por aplicações do Q do Amazon Q Business

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição de aplicações do Q do Amazon Q Business

As aplicações do Q do Amazon Q Business definem as chaves de condição a seguir que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString
qapps:AppIsPublished	Filtra o acesso de acordo com a publicação da aplicação do Q	String
qapps:SessionIsShared	Filtra o acesso de acordo com o compartilhamento da aplicação do Q	String
qapps:UserIsAppOwner	Filtra o acesso se o solicitante for proprietário da aplicação do Q	String
qapps:UserIsSessionModerator	Filtra o acesso de acordo com o fato de o solicitante ser moderador da sessão da aplicação do Q	String

Ações, recursos e chaves de condição para o Amazon Q Developer

O Amazon Q Developer (prefixo do serviço:`qdeveloper`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Q Developer
- Tipos de recursos definidos pelo Amazon Q Developer
- Chaves de condição para Amazon Q Developer

Ações definidas pelo Amazon Q Developer

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ExportArtifact	Concede permissão para exportar artefatos do Amazon Q Developer	Gravar	codeTransformation		
ImportArtifact	Concede permissão para importar artefatos para o Amazon Q Developer	Gravar	codeTransformation		
ListTagsForResource [somente permissão]	Concede permissão para listar todas as tags associadas a um recurso do Amazon Q Developer	Lista	codeTransformation		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartAgentSession	Concede permissão para iniciar uma sessão de agente com o Amazon Q Developer	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
TagResource [somente permissão]	Concede permissão para associar tags a um recurso do Amazon Q Developer	Tags	codeTransformation		
				aws:TagKeys aws:RequestTag/${TagKey}	
TransformCode	Concede permissão para transformar código com o Amazon Q Developer Transform Agent	Gravar	codeTransformation		
UntagResource [somente permissão]	Concede permissão para remover tags associadas a um recurso do Amazon Q Developer	Tags	codeTransformation		
				aws:TagKeys	

Tipos de recursos definidos pelo Amazon Q Developer

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso

também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
codeTransformation	`arn:${Partition}:qdeveloper:${Region}:${Account}:codeTransformation/${Identifier}`	aws:ResourceTag/${TagKey}

Chaves de condição para Amazon Q Developer

O Amazon Q Developer define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas tags associadas ao recurso Amazon Q Developer	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Q in Connect

O Amazon Q in Connect (prefixo do serviço: `wisdom`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Q in Connect
- Tipos de recursos definidos pelo Amazon Q in Connect
- Chaves de condição do Amazon Q in Connect

Ações definidas pelo Amazon Q in Connect

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ActivateMessageTemplate	Concede permissão para ativar um modelo de mensagem	Gravar	KnowledgeBase*		
			MessageTemplate*		
AllowVendedLogDeliveryForResource [somente permissão]	Concede permissão para configurar a entrega de logs fornecidos para um assistente	Gerenciamento de permissões	Assistant		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAIAgent	Concede permissão para criar um agente de IA	Gravar	Assistant*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateAIAgentVersion	Concede permissão para criar uma versão do agente de IA	Gravar	AIAgent*		
			Assistant*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateAIGuardrail	Concede permissão para criar uma grade de proteção aérea	Gravar	Assistant*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateAIGuardrailVersion	Concede permissão para criar uma versão de guardrail de inteligência artificial	Gravar	AIGuardrail*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			Assistant *		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateAIPrompt	Concede permissão para criar um prompt de IA	Gravar	Assistant *		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateAIPromptVersion	Concede permissão para criar uma versão do prompt de IA	Gravar	AIPrompt*		
			Assistant *		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAssistant	Concede permissão para criar um assistente	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAssistantAssociation	Concede permissão para criar uma associação entre um assistente e outro recurso	Gravar	Assistant*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateContent	Concede permissão para criar conteúdo	Gravar	KnowledgeBase*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateContentAssociation	Concede permissão para criar uma associação de conteúdo	Gravar	Content*		
			KnowledgeBase*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKnowledgeBase	Concede permissão para criar uma base de conhecimentos	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
CreateMessageTemplate	Concede permissão para criar um modelo de mensagem	Gravar	KnowledgeBase*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateMessageTemplateAttachment	Concede permissão para criar um anexo em um modelo de mensagem	Gravar	KnowledgeBase*		
			MessageTemplate*		
CreateMessageTemplateVersion	Concede permissão para criar uma versão de um modelo de mensagem	Gravar	KnowledgeBase*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			MessageTemplate*		
CreateQuickResponse	Concede permissão para criar uma resposta rápida	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
CreateSession	Concede permissão para criar uma sessão	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
DeactivateMessageTemplate	Concede permissão para desativar um modelo de mensagem	Gravar	KnowledgeBase*		
			MessageTemplate*		
DeleteAIAgent	Concede permissão para excluir um agente de IA	Gravar	AIAgent*		
			Assistant*		
DeleteAIAgentVersion	Concede permissão para excluir uma versão do agente de IA	Gravar	AIAgent*		
			Assistant*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteAIGuardrail	Concede permissão para excluir uma grade de proteção aérea	Gravar	AIGuardrail*		
			Assistant*		
DeleteAIGuardrailVersion	Concede permissão para excluir uma versão do ai guardrail	Gravar	AIGuardrail*		
			Assistant*		
DeleteAIPrompt	Concede permissão para excluir um prompt de IA	Gravar	AIPrompt*		
			Assistant*		
DeleteAIPromptVersion	Concede permissão para excluir uma versão do prompt de IA	Gravar	AIPrompt*		
			Assistant*		
DeleteAssistant	Concede permissão para excluir um assistente	Gravar	Assistant*		
DeleteAssistantAssociation	Concede permissão para excluir uma associação de assistente	Gravar	Assistant*		
			AssistantAssociation*		
DeleteContent	Concede permissão para excluir conteúdo	Gravar	Content*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			KnowledgeBase*		
DeleteContentAssociation	Concede permissão para excluir uma associação de conteúdo	Gravar	Content*		
			ContentAssociation*		
			KnowledgeBase*		
DeleteImportJob	Concede permissão para excluir um trabalho de importação de uma base de conhecimento	Gravar	KnowledgeBase*		
DeleteKnowledgeBase	Concede permissão para excluir uma base de conhecimentos	Gravar	KnowledgeBase*		
DeleteMessageTemplate	Concede permissão para excluir um modelo de mensagem	Gravar	KnowledgeBase*		
			MessageTemplate*		
DeleteMessageTemplateAttachment	Concede permissão para excluir um anexo de um modelo de mensagem	Gravar	KnowledgeBase*		
			MessageTemplate*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteQuickResponse	Concede permissão para excluir uma resposta rápida	Gravar	KnowledgeBase*		
			QuickResponse*		
GetAIAgent	Concede permissão para recuperar informações sobre um agente de IA	Leitura	AIAgent*		
			Assistant*		
GetAIGuardrail	Concede permissão para recuperar informações sobre uma grade de proteção aérea	Leitura	AIGuardrail*		
			Assistant*		
GetAIPrompt	Concede permissão para recuperar informações sobre um prompt de IA	Leitura	AIPrompt*		
			Assistant*		
GetAssistant	Concede permissão para recuperar informações sobre um assistente	Leitura	Assistant*		
GetAssistantAssociation	Concede permissão para recuperar informações sobre uma associação de assistente	Leitura	Assistant*		
			AssistantAssociation*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetContent	Concede permissão para recuperar conteúdo, incluindo um URL pré-assinado para baixar conteúdo	Leitura	Content*		
			KnowledgeBase*		
GetContentAssociation	Concede permissão para recuperar informações sobre uma associação de conteúdos	Leitura	Content*		
			ContentAssociation*		
			KnowledgeBase*		
GetContentSummary	Concede permissão para recuperar informações resumidas sobre o conteúdo	Leitura	Content*		
			KnowledgeBase*		
GetImportJob	Concede permissão para recuperar informações sobre o trabalho de importação	Leitura	KnowledgeBase*		
GetKnowledgeBase	Concede permissão para recuperar informações sobre a base de conhecimentos	Leitura	KnowledgeBase*		
GetMessageTemplate	Concede permissão para recuperar um modelo de mensagem	Leitura	KnowledgeBase*		
			MessageTemplate*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				wisdom:MessageTemplate/RoutingProfileArn	
GetNextMessage	Concede permissão para recuperar a próxima mensagem em uma sessão	Leitura	Assistant*		
			Session*		
GetQuickResponse	Concede permissão para recuperar conteúdo	Leitura	KnowledgeBase*		
			QuickResponse*		
GetRecommendations	Concede permissão para recuperar recomendações para a sessão especificada	Leitura	Assistant*		
GetSession	Concede permissão para recuperar informações para uma sessão especificada	Leitura	Assistant*		
			Session*		
ListAIAgentVersions	Concede permissão para listar informações sobre versões do agente de IA	Lista	AIAgent*		
			Assistant*		
ListAIAgents	Concede permissão para listar informações sobre agentes de IA	Lista	Assistant*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAIGuardrailVersions	Concede permissão para listar informações sobre as versões do ai guardrail	Lista	AIGuardrail*		
			Assistant*		
ListAIGuardrails	Concede permissão para listar informações sobre grades de proteção de IA	Lista	Assistant*		
ListAIPromptVersions	Concede permissão para listar informações sobre versões de prompt de IA	Lista	AIPrompt*		
			Assistant*		
ListAIPrompts	Concede permissão para listar informações sobre prompts de IA	Lista	Assistant*		
ListAssistantAssociations	Concede permissão para listar informações sobre associações de assistente	Lista			
ListAssistants	Concede permissão para listar informações sobre assistentes	Lista			
ListContentAssociations	Concede permissão para listar informações sobre associações de conteúdo	Lista	Content*		
			KnowledgeBase*		
ListContents	Concede permissão para listar o conteúdo com uma base de conhecimentos	Lista	KnowledgeBase*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListImportJobs	Concede permissão para listar informações sobre bases de conhecimentos	Lista	KnowledgeBase*		
ListKnowledgeBases	Concede permissão para listar informações sobre bases de conhecimentos	Lista			
ListMessageTemplateVersions	Concede permissão para listar versões de modelos de mensagens para o modelo de mensagem especificado	Lista	KnowledgeBase*		
			MessageTemplate*		
ListMessageTemplates	Concede permissão para listar os modelos de mensagem de uma base de conhecimentos	Lista	KnowledgeBase*		
ListMessages	Concede permissão para listar mensagens em uma sessão	Lista	Assistant*		
			Session*		
ListQuickResponses	Concede permissão para listar a resposta rápida com uma base de conhecimento	Lista	KnowledgeBase*		
ListTagsForResource	Concede permissão para listar as etiquetas para o recurso especificado	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
NotifyRecommendationsReceived	Concede permissão para remover as recomendações especificadas da fila de recomendações recém-disponíveis do assistente especificado	Gravar			
PutFeedback	Concede permissão para enviar um comentário	Gravar	Assistant*		
QueryAssistant	Concede permissão para realizar uma pesquisa manual no assistente especificado	Leitura	Assistant*		
RemoveAssistantAIAgent	Concede permissão para remover um agente de IA de um assistente	Gravar	Assistant*		
RemoveKnowledgeBaseTemplateUri	Concede permissão para remover um modelo de URI de uma base de conhecimentos	Gravar	KnowledgeBase*		
RenderMessageTemplate	Concede permissão para renderizar um modelo de mensagem	Leitura	KnowledgeBase*		wisdom:GetMessageTemplate
			MessageTemplate*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				wisdom:MessageTemplate/RoutingProfileArn	
SearchContent	Concede permissão para pesquisar conteúdo que faz referência a uma base de conhecimentos especificada. Pode ser usado para obter um recurso específico pelo nome	Leitura	KnowledgeBase*		
SearchMessageTemplates	Concede permissão para pesquisar modelos de mensagens que fazem referência a uma base de conhecimento especificada	Leitura	KnowledgeBase*		
				wisdom:SearchFilter/RoutingProfileArn wisdom:SearchFilter/Qualifier	
SearchQuickResponses	Concede permissão para procurar uma resposta rápida que faz referência a uma base de conhecimento especificada	Leitura	KnowledgeBase*		wisdom:GetQuickResponse

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				wisdom:SearchFilter/RoutingProfileArn	
SearchSessions	Concede permissão para pesquisar sessões que fazem referência a um assistente especificado. Pode ser usado para obter um recurso de sessão específico pelo nome	Leitura			
SendMessage	Concede permissão para enviar uma mensagem	Gravar	Assistant*		
			Session*		
StartContentUpload	Concede permissão para obter um URL para carregar conteúdo para uma base de conhecimentos	Gravar	KnowledgeBase*		
StartImportJob	Concede permissão para criar várias respostas rápidas	Gravar	KnowledgeBase*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para adicionar as etiquetas especificadas ao recurso especificado	Tags	Assistant		
			Assistant Association		
			Content		
			ContentAssociation		
			KnowledgeBase		
			MessageTemplate		
			QuickResponse		
			Session		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource		Tags	Assistant		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	Concede permissão para remover as etiquetas especificadas do recurso especificado		Assistant Association		
			Content		
			ContentAssociation		
			KnowledgeBase		
			MessageTemplate		
			QuickResponse		
			Session		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateAIAgent	Concede permissão para atualizar informações sobre um agente de IA	Gravar	AIAgent*		
			Assistant*		
UpdateAIGuardrail	Concede permissão para atualizar informações sobre uma grade de proteção aérea	Gravar	AIGuardrail*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			Assistant*		
UpdateAIPrompt	Concede permissão para atualizar informações sobre um prompt de IA	Gravar	AIPrompt*		
			Assistant*		
UpdateAssistantAIAgent	Concede permissão para atualizar informações do assistente sobre um agente de IA	Gravar	Assistant*		
UpdateContent	Concede permissão para atualizar as informações sobre o conteúdo	Gravar	Content*		
			KnowledgeBase*		
UpdateKnowledgeBaseTemplateUri	Concede permissão para atualizar um modelo de URI de uma base de conhecimentos	Gravar	KnowledgeBase*		
UpdateMessageTemplate	Concede permissão para atualizar o conteúdo do modelo de mensagem	Gravar	KnowledgeBase*		
			MessageTemplate*		
UpdateMessageTemplateMetadata	Concede permissão para atualizar os metadados do modelo de mensagem	Gravar	KnowledgeBase*		
			MessageTemplate*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateQuickResponse	Concede permissão para atualizar informações ou conteúdo sobre a resposta rápida	Gravar	KnowledgeBase*		
			QuickResponse*		
UpdateSession	Concede permissão para atualizar uma sessão	Gravar	Assistant*		
			Session*		
UpdateSessionData	Concede permissão para atualizar dados armazenados em uma sessão	Gravar	Assistant*		
			Session*		

Tipos de recursos definidos pelo Amazon Q in Connect

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
AIAgent	`arn:${Partition}:wisdom:${Region}:${Account}:ai-agent/${AssistantId}/${AIAgentId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
AIPrompt	arn:${Partition}:wisdom:${Region}:${Account}:ai-prompt/${AssistantId}/${AIPromptId}	aws:ResourceTag/${TagKey}
AIGuardrail	arn:${Partition}:wisdom:${Region}:${Account}:ai-guardrail/${AssistantId}/${AIGuardrailId}	aws:ResourceTag/${TagKey}
Assistant	arn:${Partition}:wisdom:${Region}:${Account}:assistant/${AssistantId}	aws:ResourceTag/${TagKey}
Assistant Association	arn:${Partition}:wisdom:${Region}:${Account}:association/${AssistantId}/${AssistantAssociationId}	aws:ResourceTag/${TagKey}
Content	arn:${Partition}:wisdom:${Region}:${Account}:content/${KnowledgeBaseId}/${ContentId}	aws:ResourceTag/${TagKey}
ContentAssociation	arn:${Partition}:wisdom:${Region}:${Account}:content-association/${KnowledgeBaseId}/${ContentId}/${ContentAssociationId}	aws:ResourceTag/${TagKey}
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

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do Amazon Q in Connect

O Amazon Q in Connect define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString
wisdom:MessageTemplate/	Filtra o acesso pelos ARNs do perfil de roteamento de conexão associados ao recurso	ArrayOfARN

Chaves de condição	Descrição	Tipo
RoutingProfileArn		
wisdom:SearchFilter/Qualifier	Filtra o acesso pelos qualificadores que são transmitidos na solicitação	ArrayOfString
wisdom:SearchFilter/RoutingProfileArn	Filtra o acesso pelo ARN do perfil do roteamento de conexão que é passado na solicitação	ARN

Ações, recursos e chaves de condição do Amazon QLDB

O Amazon QLDB (prefixo do serviço: `qldb`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissões do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon QLDB
- Tipos de recursos definidos pelo Amazon QLDB
- Chaves de condição do Amazon QLDB

Ações definidas pelo Amazon QLDB

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou

ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelJournalKinesisStream	Concede permissão para cancelar um streaming kinesis de diário	Write	stream*		
CreateLedger	Concede permissão para criar um livro contábil	Write	ledger*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteLedger	Concede permissão para excluir um livro contábil	Write	ledger*		
DescribeJournalKinesisStream	Concede permissão para descrever informações sobre um streaming kinesis de diário	Read	stream*		
DescribeJournalS3Export	Concede permissão para descrever informações sobre um trabalho de exportação de diário	Read	ledger*		
DescribeLedger	Concede permissão para descrever um livro contábil	Leitura	ledger*		
ExecuteStatement [somente permissão]	Concede permissão para enviar comandos para um livro contábil por meio do console	Write	ledger*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ExportJournalToS3	Concede permissão para exportar o conteúdo do diário para um bucket do Amazon S3	Gravar	ledger*		
GetBlock	Concede permissão para recuperar um bloco de um livro contábil para um determinado BlockAddress	Leitura	ledger*		
GetDigest	Concede permissão para recuperar um resumo de um livro contábil para um determinado BlockAddress	Leitura	ledger*		
GetRevision	Concede permissão para recuperar uma revisão para um determinado ID de documento e um determinado BlockAddress	Leitura	ledger*		
InsertSampleData [somente permissão]	Concede permissão para inserir exemplos de dados de aplicativo por meio do console	Write	ledger*		
ListJournalKinesisStreamsForLedger	Concede permissão para listar streamings kinesis de diário para um livro contábil especificado	List	stream*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListJournalS3Exports	Concede permissão para listar trabalhos de exportação de diário para todos os livros contábeis	List			
ListJournalS3ExportsForLedger	Concede permissão para listar trabalhos de exportação de diário para um livro contábil especificado	List	ledger*		
ListLedgers	Concede permissão para listar livros contábeis existentes	List			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Read	catalog		
			ledger		
			stream		
			table		
PartiQLCreateIndex	Concede permissão para criar um índice em uma tabela	Write	table*		
PartiQLCreateTable	Concede permissão para criar uma tabela	Write	table*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PartiQLDelete	Concede permissão para excluir documentos de uma tabela	Write	table*		
PartiQLDropIndex	Concede permissão para remover um índice de uma tabela	Write	table*		
				qldb:Purge	
PartiQLDropTable	Concede permissão para remover uma tabela	Write	table*		
				qldb:Purge	
PartiQLHistoryFunction	Concede permissão para usar a função de histórico em uma tabela	Read	table*		
PartiQLInsert	Concede permissão para inserir documentos em uma tabela	Gravar	table*		
PartiQLRedact	Concede permissão para editar revisões históricas	Gravar	table*		
PartiQLSelect	Concede permissão para selecionar documentos de uma tabela	Read	catalog		
			table		
PartiQLUndropTable	Concede permissão para cancelar a remoção de uma tabela	Write	table*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PartiQLUpdate	Concede permissão para atualizar documentos existentes em uma tabela	Write	table*		
SendCommand	Concede permissão para enviar comandos a um livro contábil	Gravar	ledger*		
ShowCatalog [somente permissão]	Concede permissão para visualizar o catálogo de um livro contábil por meio do console	Write	ledger*		
StreamJournalToKinesis	Concede permissão para fazer streaming do conteúdo do diário para um stream de dados do Kinesis	Write	stream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Concede permissão para adicionar uma ou mais etiquetas a um recurso	Marcação	catalog		
			ledger		
			stream		
			table		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover uma ou mais etiquetas de um recurso	Marcação	catalog		
			ledger		
			stream		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateLedger	Concede permissão para atualizar propriedades em um livro contábil	Write	ledger*		
UpdateLedgerPermissionsMode	Concede permissão para atualizar o modo de permissões em um livro-razão	Write	ledger*		

Tipos de recursos definidos pelo Amazon QLDB

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações

identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do Amazon QLDB

O Amazon QLDB define as chaves de condição a seguir que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por um par de chave valor da etiqueta que é permitido na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso por um par de chave e valor da etiqueta de um recurso.	Segmento
aws:TagKeys	Filtra o acesso por uma lista de chaves da etiqueta que são permitidas na solicitação	ArrayOfString
qldb:Purge	Filtra o acesso pelo valor de purga especificado em uma instrução DROP (Retirar) do PartiQL	String

Ações, recursos e chaves de condição para a Amazon QuickSight

A Amazon QuickSight (prefixo do serviço:`quicksight`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon QuickSight
- Tipos de recursos definidos pela Amazon QuickSight
- Chaves de condição para a Amazon QuickSight

Ações definidas pela Amazon QuickSight

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando

usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AccountConfigurations [somente permissão]	Concede permissão para ativar a configuração do acesso padrão aos AWS recursos	Gravar			
BatchCreateTopicReviewedAnswer	Concede permissão para criar respostas revisadas para um tópico	Gravar	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
BatchDeleteTopicReviewedAnswer	Concede permissão para excluir respostas revisadas de um tópico	Gravar	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CancelIngestion	Concede permissão para cancelar ingestões de SPICE em um conjunto de dados	Gravar	ingestion*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAccountCustomization	Concede permissão para criar uma personalização de conta para QuickSight conta ou namespace	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAccountSubscription	Concede permissão para assinar QuickSight	Gravar		quicksight:Edition quicksight:DirectoryType	
CreateAdmin [somente permissão]	Concede permissão para provisionar QuickSight administradores, autores e leitores da Amazon	Gravar	user*		
CreateAnalysis	Concede permissão para criar uma análise a partir de um modelo	Gravar	analysis*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBrand	Concede permissão para criar uma QuickSight marca da Amazon	Gravar	brand*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomPermissions	Concede permissão para criar um recurso de permissões QuickSight personalizadas	Gravar	custompermissions*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDashboard	Concede permissão para criar um QuickSight painel	Gravar	dashboard*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSet	Concede permissão para criar um conjunto de dados	Write	datasource*		quicksight:PassDataSource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSource	Concede permissão para criar uma fonte de dados	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
CreateEmailCustomizationTemplate [somente permissão]	Concede permissão para criar um modelo de personalização de QuickSight e-mail	Gravar	emailCustomizationTemplate*		
CreateFolder	Concede permissão para criar uma QuickSight pasta	Gravar	folder*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFolderMembership	Concede permissão para adicionar um QuickSight painel, análise ou conjunto de dados a uma pasta QuickSight	Gravar	folder*		
			analysis		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			dashboard		
			dataset		
CreateGroup	Concede permissão para criar um QuickSight grupo	Gravar	group*		
CreateGroupMembership	Concede permissão para adicionar um QuickSight usuário a um QuickSight grupo	Gravar	group*	quicksight:UserName	
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateIAMPolicyAssignment	Concede permissão para criar um exercício com um ARN de política do IAM especificado que será atribuído a grupos ou usuários específicos do QuickSight	Gravar	assignment*		
CreateIngestion	Concede permissão para iniciar uma ingestão de SPICE em um conjunto de dados	Gravar	ingestion*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateNamespace	Concede permissão para criar um QuickSight namespace	Gravar	namespace*		ds:CreateIdentityPoolDirectory
CreateReader [somente permissão]	Concede permissão para provisionar QuickSight leitores da Amazon	Gravar	user*		
CreateRefreshSchedule	Concede permissão para criar uma programação de atualização de um conjunto de dados	Gravar	refreshschedule*		
CreateRoleMembership	Concede permissão para adicionar um membro de grupo a um perfil	Gravar		quicksight:Group	
CreateTemplate	Concede permissão para criar um modelo	Write	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTemplateAlias	Concede permissão para criar um alias de modelo	Gravar	template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTheme	Concede permissão para criar um tema	Gravar	theme*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateThemeAlias	Concede permissão para criar um alias para uma versão de tema	Gravar	theme*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTopic	Concede permissão para criar um tópico	Gravar	dataset*		quicksight:PassDataSet

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTopicRefreshSchedule	Concede permissão para criar uma programação de atualização para um tópico	Gravar	topic*		
CreateUser [somente permissão]	Concede permissão para provisionar QuickSight autores e leitores da Amazon	Gravar	user*		
CreateVPCConnection	Concede permissão para criar uma conexão de vpc	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
DeleteAccountCustomization	Concede permissão para excluir uma personalização de conta para QuickSight conta ou namespace	Gravar	customization*		
DeleteAccountSubscription	Concede permissão para excluir uma QuickSight conta	Gravar	account*		
DeleteAnalysis	Concede permissão para excluir uma análise	Gravar	analysis*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteBrand	Concede permissão para excluir uma QuickSight marca da Amazon	Gravar	brand*		
DeleteBrandAssignment	Concede permissão para excluir uma atribuição de marca	Gravar			
DeleteCustomPermissions	Concede permissão para excluir um recurso de permissões QuickSight personalizadas	Gravar			
DeleteDashboard	Concede permissão para excluir um QuickSight painel	Gravar	dashboard*		
DeleteDataSet	Concede permissão para excluir um conjunto de dados	Gravar	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDataSetRefreshProperties	Concede permissão para excluir propriedades de atualização do conjunto de dados de um conjunto de dados	Gravar	dataset*		
DeleteDataSource	Concede permissão para excluir uma fonte de dados	Gravar	datasource*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDefaultQBusinessApplication	Concede permissão para excluir o QBusiness aplicativo vinculado à QuickSight conta	Gravar			
DeleteEmailCustomizationTemplate [somente permissão]	Concede permissão para excluir um modelo de personalização de QuickSight e-mail	Gravar	emailCustomizationTemplate*		
DeleteFolder	Concede permissão para excluir uma QuickSight pasta	Gravar	folder*		
DeleteFolderMembership	Concede permissão para remover um QuickSight painel, análise ou conjunto de dados de uma pasta QuickSight	Gravar	folder*		
			analysis		
			dashboard		
			dataset		
DeleteGroup	Concede permissão para remover um grupo de usuários do QuickSight	Gravar	group*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteGroupMembership	Concede permissão para remover um usuário de um grupo para que ele não he/she seja mais membro do grupo	Gravar	group*	quicksight:UserName	
DeleteIAMPolicyAssignment	Concede permissão para atualizar uma atribuição existente	Gravar	assignment*		
DeleteIdentityPropagationConfig	Concede permissão para remover AWS serviços de propagação de identidade confiável no QuickSight	Gravar			
DeleteNamespace	Concede permissão para excluir um QuickSight namespace	Gravar	namespace*		ds:DeleteDirectory
DeleteRefreshSchedule	Concede permissão para excluir uma programação de atualização de um conjunto de dados	Gravar	refreshschedule*		
DeleteRoleCustomPermission	Concede permissão para remover a permissão personalizada associada a um perfil	Gravar			
DeleteRoleMembership	Concede permissão para remover um membro de grupo de um perfil	Gravar		quicksight:Group	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteTemplate	Concede permissão para excluir um modelo	Write	template*		
DeleteTemplateAlias	Concede permissão para excluir um alias de modelo	Write	template*		
DeleteTheme	Concede permissão para excluir um tema	Write	theme*		
DeleteThemeAlias	Concede permissão para excluir o alias de um tema	Gravar	theme*		
DeleteTopic	Concede permissão para excluir um tópico	Gravar	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteTopicRefreshSchedule	Concede permissão para excluir uma programação de atualização de um tópico	Gravar	topic*		
DeleteUser	Concede permissão para excluir um QuickSight usuário, dado o nome do usuário	Gravar	user*		
DeleteUserByPrincipalId	Concede permissão para excluir um usuário identificado por sua ID principal	Gravar	user*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteUserCustomPermission	Concede permissão para remover a permissão personalizada associada a um usuário	Gravar	user*		
DeleteVPCConnection	Concede permissão para excluir uma conexão de vpc	Gravar	vpcconnection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeAccountCustomization	Concede permissão para descrever uma personalização de conta para QuickSight conta ou namespace	Leitura	customization*		
DescribeAccountSettings	Concede permissão para descrever as configurações administrativas da QuickSight conta	Leitura			
DescribeAccountSubscription	Concede permissão para descrever uma QuickSight conta	Leitura	account*		
DescribeAnalysis	Concede permissão para descrever uma análise	Leitura	analysis*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeAnalysisPermissions	Concede permissão para descrever permissões para uma análise	Leitura	analysis*		
DescribeAssetBundleExportJob	Concede permissão para descrever um trabalho de exportação de pacote de recursos	Leitura	assetBundleExportJob*		
DescribeAssetBundleImportJob	Concede permissão para descrever um trabalho de importação de pacote de recursos	Leitura	assetBundleImportJob*		
DescribeBrand	Concede permissão para descrever uma marca	Leitura	brand*		
DescribeBrandAssignment	Concede permissão para descrever uma atribuição de marca	Leitura			
DescribeBrandPublishedVersion	Concede permissão para descrever a versão publicada da marca	Leitura	brand*		
DescribeCustomPermissions	Concede permissão para descrever um recurso de permissões personalizadas em uma QuickSight conta	Leitura	custompermissions*		
DescribeDashboard	Concede permissão para descrever um QuickSight painel	Leitura	dashboard*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeDashboardPermissions	Concede permissão para descrever permissões para um QuickSight painel	Leitura	dashboard*		
DescribeDashboardSnapshotJob	Concede permissão para descrever um trabalho de snapshot de painel	Leitura	dashboardSnapshotJob*		
DescribeDashboardSnapshotJobResult	Concede permissão para descrever o resultado de um trabalho de snapshot de painel	Leitura	dashboardSnapshotJob*		
DescribeDashboardsQAConfiguration	Concede permissão para descrever uma configuração de painéis	Leitura			
DescribeDataSet	Concede permissão para descrever um conjunto de dados	Leitura	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeDataSetPermissions	Concede permissão para descrever a política de recursos de um conjunto de dados	Gerenciamento de permissões	dataset*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeDataSetRefreshProperties	Concede permissão para descrever propriedades de atualização de um conjunto de dados	Leitura	dataset*		
DescribeDataSource	Concede permissão para descrever uma fonte de dados	Leitura	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeDataSourcePermissions	Concede permissão para descrever a política de recursos de uma fonte de dados	Gerenciamento de permissões	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeDefaultQBusinessApplication	Concede permissão para descrever o ID QBusiness do aplicativo vinculado à QuickSight conta	Leitura			
DescribeEmailCustomizationTemplate [somente permissão]	Concede permissão para descrever um modelo de personalização de QuickSight e-mail	Leitura	emailCustomizationTemplate*		
DescribeFolder	Concede permissão para descrever uma QuickSight pasta	Leitura	folder*		
DescribeFolderPermissions	Concede permissão para descrever permissões para uma QuickSight pasta	Leitura	folder*		
DescribeFolderResolvedPermissions	Concede permissão para descrever as permissões resolvidas para uma QuickSight pasta	Leitura	folder*		
DescribeGroup	Concede permissão para descrever um QuickSight grupo	Leitura	group*		
DescribeGroupMembership	Concede permissão para descrever um membro QuickSight do grupo	Leitura	group*	quicksight:UserName	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeIAMPolicyAssignment	Concede permissão para descrever uma atribuição existente	Leitura	assignment*		
DescribeIngestion	Concede permissão para descrever uma ingestão de SPICE em um conjunto de dados	Leitura	ingestion*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeIpRestriction	Concede permissão para descrever as restrições de IP QuickSight da conta	Leitura			
DescribeKeyRegistration	Concede permissão para descrever o registro da QuickSight chave	Leitura			
DescribeNamespace	Concede permissão para descrever um QuickSight namespace	Leitura	namespace*		
DescribeQPersonalizationConfiguration	Concede permissão para descrever uma configuração de personalização	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeQuickSightQSearchConfiguration	Concede permissão para descrever a configuração do QuickSight Q Search	Leitura			
DescribeRefreshSchedule	Concede permissão para descrever uma programação de atualização de um conjunto de dados	Leitura	refreshschedule*		
DescribeRoleCustomPermission	Concede permissão para descrever a permissão personalizada associada a um perfil	Leitura			
DescribeTemplate	Concede permissão para descrever um modelo	Leitura	template*		
DescribeTemplateAlias	Concede permissão para descrever um alias de modelo	Leitura	template*		
DescribeTemplatePermissions	Concede permissão para descrever permissões para um modelo	Leitura	template*		
DescribeTheme	Concede permissão para descrever um tema	Leitura	theme*		
DescribeThemeAlias	Concede permissão para descrever um alias de tema	Leitura	theme*		
DescribeThemePermissions	Concede permissão para descrever permissões para um tema	Leitura	theme*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeTopic	Concede permissão para descrever um tópico	Leitura	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeTopicPermissions	Concede permissão para descrever a política de recursos de um tópico	Gerenciamento de permissões	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeTopicRefresh	Concede permissão para descrever o status de atualização de um tópico	Leitura	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeTopicRefreshSchedule	Concede permissão para descrever a programação de atualização de um tópico	Leitura	topic*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeUser	Concede permissão para descrever um QuickSight usuário com o nome de usuário	Leitura	user*		
DescribeVPCConnection	Concede permissão para descrever uma conexão de vpc	Leitura	vpcconnection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GenerateEmbedUrlForAnonymousUser	Concede permissão para gerar um URL usado para incorporar um QuickSight painel ou um tópico para um usuário não registrado no QuickSight	Gravar	namespace*		
			dashboard		
			theme		
			topic		
				quicksight:AllowedEmbeddingDomains	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GenerateEmbedUrlForRegisteredUser	Concede permissão para gerar um URL usado para incorporar um QuickSight painel para um usuário registrado no QuickSight	Gravar	user*		
				quicksight:AllowedEmbeddingDomains	
GenerateEmbedUrlForRegisteredUserWithIdentity	Concede permissão para gerar um URL usado para incorporar uma QuickSight experiência para um usuário registrado QuickSight usando a sessão de função aprimorada por identidade	Gravar		quicksight:AllowedEmbeddingDomains	
GetAnonymousUserEmbedUrl [somente permissão]	Concede permissão para obter um URL usado para incorporar um QuickSight painel para um usuário não registrado no QuickSight	Leitura			
GetAuthCode [somente permissão]	Concede permissão para obter um código de autenticação representando um usuário QuickSight	Leitura	user*		
GetDashboardEmbedUrl	Concede permissão para obter um URL usado para incorporar um painel QuickSight	Leitura	dashboard*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetGroupMapping [somente permissão]	Concede permissão para usar a Amazon QuickSight, na edição Enterprise, para identificar e exibir os grupos de diretórios do Microsoft Active Directory (Microsoft Active Directory) que estão mapeados para funções na Amazon QuickSight	Leitura			
GetSessionEmbedUrl	Concede permissão para obter um URL para incorporar a experiência QuickSight do console	Leitura			
ListAnalyses	Concede permissão para listar todas as análises em uma conta	Listar	analysis*		
ListAssetBundleExportJobs	Concede permissão para listar todos os trabalhos de exportação de pacote de recursos	Lista	assetBundleExportJob*		
ListAssetBundleImportJobs	Concede permissão para listar todos os trabalhos de importação de pacote de recursos	Lista	assetBundleImportJob*		
ListBrands	Concede permissão para listar todas as marcas em uma QuickSight conta da Amazon	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListCustomPermissions	Concede permissão para listar recursos de permissões personalizadas na QuickSight conta	Lista			
ListCustomerManagedKeys [somente permissão]	Concede permissão para listar todas as chaves gerenciadas do cliente registradas	Lista			
ListDashboardVersions	Concede permissão para listar todas as versões de um QuickSight painel	Lista	dashboard*		
ListDashboards	Concede permissão para listar todos os painéis em uma conta QuickSight	Lista	dashboard*		
ListDataSets	Concede permissão para listar todos os conjuntos de dados	Listar		aws:RequestTag/${TagKey} aws:TagKeys	
ListDataSources	Concede permissão para listar todas as fontes de dados	Lista		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListFolderMembers	Concede permissão para listar todos os membros em uma pasta	Leitura	folder*		
ListFolders	Concede permissão para listar todas as pastas em uma QuickSight conta	Lista	folder*		
ListFoldersForResource	Concede permissão para listar todas as pastas das quais um QuickSight recurso é membro	Lista	analysis		
			dashboard		
			dataset		
			datasource		
			topic		
ListGroupMemberships	Concede permissão para listar usuários membros em um grupo	Lista	group*		
ListGroups	Concede permissão para listar todos os grupos de usuários no QuickSight	Lista	group*		
ListIAMPolicyAssignments	Concede permissão para listar todas as tarefas na conta atual da Amazon QuickSight	Lista	assignment*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListIAMPolicyAssignmentsForUser	Concede permissão para listar todas as atribuições atribuídas a um usuário e aos grupos que pertence	Lista	assignment*		
ListIdentityPropagationConfigs	Concede permissão para listar AWS serviços habilitados para propagação de identidade confiável no QuickSight	Lista			
ListIngestions	Concede permissão para listar todas as ingestões de SPICE em um conjunto de dados	Lista		aws:RequestTag/${TagKey} aws:TagKeys	
ListKMSKeysForUser [somente permissão]	Concede permissão para listar chaves do KMS de um usuário	Lista			
ListNamespaces	Concede permissão para listar todos os namespaces em uma conta QuickSight	Lista			
ListRefreshSchedules	Concede permissão para listar todos os programaçãos de atualização de um conjunto de dados	Lista			
ListRoleMemberships	Concede permissão para listar os membros de um perfil	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar as tags de um QuickSight recurso	Leitura	analysis		
			brand		
			customization		
			custompermissions		
			dashboard		
			dataset		
			datasource		
			folder		
			template		
			theme		
			topic		
			vpcconnection		
ListTemplateAliases	Concede permissão para listar todas as etiquetas de um recurso	Listar	template*		
ListTemplateVersions	Concede permissão para listar todas as versões de um modelo	Lista	template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTemplates	Concede permissão para listar todos os modelos em uma QuickSight conta	Lista	template*		
ListThemeAliases	Concede permissão para listar todos os aliases de um tema	Listar	theme*		
ListThemeVersions	Concede permissão para listar todas as versões de um tema	Listar	theme*		
ListThemes	Concede permissão para listar todos os temas em uma conta	Lista	theme*		
ListTopicRefreshSchedules	Concede permissão para listar todos os programaçãos de atualização de um tópico	Lista			
ListTopicReviewedAnswers	Concede permissão para listar todas as respostas revisadas de um tópico	Lista		aws:RequestTag/${TagKey} aws:TagKeys	
ListTopics	Concede permissão para listar todos os tópicos	Lista		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListUserGroups	Concede permissão para listar grupos dos quais um determinado usuário é um membro	Lista	user*		
ListUsers	Concede permissão para listar todos os QuickSight usuários pertencentes a essa conta	Lista	user*		
ListVPCConnections	Concede permissão para listar todas as conexões de vpc	Lista		aws:RequestTag/${TagKey} aws:TagKeys	
PassDataSet [somente permissão]	Concede permissão para usar um conjunto de dados para um modelo	Leitura	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PassDataSource [somente permissão]	Concede permissão para usar uma fonte de dados para um conjunto de dados	Leitura	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PredictQAResults	Concede permissão para prever resultados de controle de qualidade	Leitura	dashboard		
			topic		
PutDataSetRefreshProperties	Concede permissão para colocar propriedades de atualização do conjunto de dados de um conjunto de dados	Gravar	dataset*		
RegisterCustomerManagedKey [somente permissão]	Concede permissão para registrar uma chave gerenciada pelo cliente	Gravar			
RegisterUser	Concede permissão para criar um QuickSight usuário, cuja identidade está associada ao IAM identity/role especificado na solicitação	Gravar	user*	quicksight:IamArn quicksight:SessionName	
RemoveCustomerManagedKey [somente permissão]	Concede permissão para remover uma chave gerenciada pelo cliente	Gravar			
RestoreAnalysis	Concede permissão para restaurar uma análise excluída	Gravar	analysis*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ScopeDownPolicy [somente permissão]	Concede permissão para gerenciar políticas de escopo para AWS permissões de recursos	Gravar			
SearchAnalyses	Concede permissão para procurar um subconjunto de análises	Lista	analysis*		
SearchDashboards	Concede permissão para pesquisar um subconjunto de painéis QuickSight	Lista	dashboard*		
SearchDataSets	Concede permissão para pesquisar um subconjunto de QuickSight DatSets	Lista	dataset*		
SearchDataSources	Concede permissão para pesquisar um subconjunto de fontes de QuickSight dados	Lista	datasource*		
SearchDirectoryGroups [somente permissão]	Concede permissão para usar a Amazon QuickSight, na edição Enterprise, para exibir seus grupos de diretórios do Microsoft Active Directory para que você possa escolher quais mapear para funções na Amazon QuickSight	Lista			
SearchFolders	Concede permissão para pesquisar um subconjunto de pastas QuickSight	Leitura	folder*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SearchGroups	Concede permissão para pesquisar um subconjunto de grupos QuickSight	Lista	group*		
SearchTopics	Concede permissão para pesquisar um subconjunto de tópicos	Lista	topic*		
SearchUsers [somente permissão]	Concede permissão para pesquisar os QuickSight usuários pertencentes a essa conta	Lista	user*		
SetGroupMapping [somente permissão]	Concede permissão para usar a Amazon QuickSight, na edição Enterprise, para exibir seus grupos de diretórios do Microsoft Active Directory para que você possa escolher quais mapear para funções na Amazon QuickSight	Gravar			
StartAssetBundleExportJob	Concede permissão para iniciar um trabalho de exportação de pacote de recursos	Gravar	assetBundleExportJob*		
StartAssetBundleImportJob	Concede permissão para iniciar um trabalho de importação de pacote de recursos	Gravar	assetBundleImportJob*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartDashboardSnapshotJob	Concede permissão para iniciar um trabalho de snapshot de painel	Gravar	dashboardSnapshotJob*		
StartDashboardSnapshotJobSchedule	Concede permissão para iniciar um agendamento de trabalho de snapshot do painel	Gravar			
Subscribe [somente permissão]	Concede permissão para assinar a Amazon QuickSight e também permite que o usuário atualize a assinatura para a edição Enterprise	Gravar		quicksight:Edition quicksight:DirectoryType	
TagResource	Concede permissão para adicionar tags a um QuickSight recurso	Tags	analysis		
			brand		
			customization		
			custompermissions		
			dashboard		
			dataset		
			datasource		
			folder		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			ingestion		
			template		
			theme		
			topic		
			vpcconnection		
				aws:TagKeys aws:RequestTag/${TagKey}	
Unsubscribe [somente permissão]	Concede permissão para cancelar a assinatura da Amazon QuickSight, o que exclui permanentemente todos os usuários e seus recursos da Amazon QuickSight	Gravar			
UntagResource	Concede permissão para remover tags de um QuickSight recurso	Tags	analysis		
			brand		
			customization		
			custompermissions		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			dashboard		
			dataset		
			datasource		
			folder		
			ingestion		
			template		
			theme		
			topic		
			vpcconnection		
				aws:TagKeys	
UpdateAccountCustomization	Concede permissão para atualizar uma personalização de conta para QuickSight conta ou namespace	Gravar	customization*		
UpdateAccountSettings	Concede permissão para atualizar as configurações administrativas da QuickSight conta	Gravar			
UpdateAnalysis	Concede permissão para atualizar uma análise	Write	analysis*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateAnalysisPermissions	Concede permissão para atualizar permissões para uma análise	Gerenciamento de permissões	analysis*		
UpdateApplicationWithTokenExchangeGrant	Concede permissão para atualizar o aplicativo QuickSight IAM Identity Center com a concessão do Token Exchange	Gravar			
UpdateBrand	Concede permissão para atualizar uma marca	Gravar	brand*		
UpdateBrandAssignment	Concede permissão para atualizar uma atribuição de marca	Gravar			
UpdateBrandPublishedVersion	Concede permissão para atualizar a versão publicada de uma marca	Gravar	brand*		
UpdateCustomPermissions	Concede permissão para atualizar um recurso de permissões QuickSight personalizadas	Gravar	custompermissions*		
UpdateDashboard	Concede permissão para atualizar um QuickSight painel	Gravar	dashboard*		
UpdateDashboardLinks	Concede permissão para atualizar os links de um QuickSight painel	Gravar	dashboard*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateDashboardPermissions	Concede permissão para atualizar as permissões de um QuickSight painel	Gerenciamento de permissões	dashboard*		
UpdateDashboardPublishedVersion	Concede permissão para atualizar a versão publicada de um QuickSight painel	Gravar	dashboard*		
UpdateDashboardsQAConfiguration	Concede permissão para atualizar a configuração dos painéis	Gravar			
UpdateDataSet	Concede permissão para atualizar um conjunto de dados	Write	dataset*		quicksight:PassDataSource
			datasource		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateDataSetPermissions	Concede permissão para atualizar a política de recursos de um conjunto de dados	Permissions management	dataset*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateDataSource	Concede permissão para atualizar uma fonte de dados	Write	datasource*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateDataSourcePermissions	Concede permissão para atualizar a política de recursos de uma fonte de dados	Gerenciamento de permissões	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateDefaultQBusinessApplication	Concede permissão para atualizar o ID QBusiness do aplicativo vinculado à QuickSight conta	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateEmailCustomizationTemplate [somente permissão]	Concede permissão para atualizar um modelo de personalização de QuickSight e-mail	Gravar	emailCustomizationTemplate*		
UpdateFolder	Concede permissão para atualizar uma QuickSight pasta	Gravar	folder*		
UpdateFolderPermissions	Concede permissão para atualizar as permissões de uma QuickSight pasta	Gerenciamento de permissões	folder*		
UpdateGroup	Concede permissão para alterar a descrição do grupo	Write	group*		
UpdateIAMPolicyAssignment	Concede permissão para atualizar uma atribuição existente	Gravar	assignment*		
UpdateIdentityPropagationConfig	Concede permissão para adicionar e atualizar AWS serviços para propagação de identidade confiável no QuickSight	Gravar			
UpdateIpRestriction	Concede permissão para atualizar as restrições de IP QuickSight da conta	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateKeyRegistration	Concede permissão para atualizar o registro da QuickSight chave	Gravar			
UpdatePublicSharingSettings	Concede permissão para habilitar ou desabilitar compartilhamento público em uma conta	Gravar			
UpdateQPersonalizationConfiguration	Concede permissão para atualizar uma configuração de personalização	Gravar			
UpdateQuickSightQSearchConfiguration	Concede permissão para atualizar a configuração do QuickSight Q Search	Gravar			
UpdateRefreshSchedule	Concede permissão para atualizar uma programação de atualização de um conjunto de dados	Gravar	refreshschedule*		
UpdateResourcePermissions [somente permissão]	Concede permissão para atualizar as permissões em nível de recurso no QuickSight	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateRoleCustomPermission	Concede permissão para atualizar a permissão personalizada associada a um perfil	Gravar			
UpdateSPICECapacityConfiguration	Concede permissão para atualizar a configuração de capacidade QuickSight do SPICE	Gravar			
UpdateTemplate	Concede permissão para atualizar um modelo	Write	template*		
UpdateTemplateAlias	Concede permissão para atualizar um alias de modelo	Write	template*		
UpdateTemplatePermissions	Concede permissão para atualizar permissões para um modelo	Permissions management	template*		
UpdateTheme	Concede permissão para atualizar um tema	Write	theme*		
UpdateThemeAlias	Concede permissão para atualizar o alias de um tema	Write	theme*		
UpdateThemePermissions	Concede permissão para atualizar permissões para um tema	Gerenciamento de permissões	theme*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateTopic	Concede permissão para atualizar um tópico	Gravar	topic*		quicksight:PassDataSet
			dataset		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTopicPermissions	Concede permissão para atualizar a política de recursos de um tópico	Gerenciamento de permissões	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTopicRefreshSchedule	Concede permissão para atualizar uma programação de atualização de um tópico	Gravar	topic*		
UpdateUser	Concede permissão para atualizar um QuickSight usuário da Amazon	Gravar	user*		
UpdateUserCustomPermission	Concede permissão para atualizar a permissão personalizada associada a um usuário	Gravar	user*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateVPCConnection	Concede permissão para atualizar uma conexão de vpc	Gravar	vpcconnection*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	

Tipos de recursos definidos pela Amazon QuickSight

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
account	`arn:${Partition}:quicksight:${Region}:${Account}:account/${ResourceId}`	
user	`arn:${Partition}:quicksight:${Region}:${Account}:user/${ResourceId}`	
group	`arn:${Partition}:quicksight:${Region}:${Account}:group/${ResourceId}`	

Tipos de recursos	ARN	Chaves de condição
analysis	arn:${Partition}:quicksight:${Region}:${Account}:analysis/${ResourceId}	aws:ResourceTag/${TagKey}
dashboard	arn:${Partition}:quicksight:${Region}:${Account}:dashboard/${ResourceId}	aws:ResourceTag/${TagKey}
template	arn:${Partition}:quicksight:${Region}:${Account}:template/${ResourceId}	aws:ResourceTag/${TagKey}
vpcconnection	arn:${Partition}:quicksight:${Region}:${Account}:vpcConnection/${ResourceId}	aws:ResourceTag/${TagKey}
assetBundleExportJob	arn:${Partition}:quicksight:${Region}:${Account}:asset-bundle-export-job/${ResourceId}	
assetBundleImportJob	arn:${Partition}:quicksight:${Region}:${Account}:asset-bundle-import-job/${ResourceId}	
datasource	arn:${Partition}:quicksight:${Region}:${Account}:datasource/${ResourceId}	aws:ResourceTag/${TagKey}
dataset	arn:${Partition}:quicksight:${Region}:${Account}:dataset/${ResourceId}	aws:ResourceTag/${TagKey}
ingestion	arn:${Partition}:quicksight:${Region}:${Account}:dataset/${DatasetId}/ingestion/${ResourceId}	aws:ResourceTag/${TagKey}
refreshschedule	arn:${Partition}:quicksight:${Region}:${Account}:dataset/${DatasetId}/refresh-schedule/${ResourceId}	

Tipos de recursos	ARN	Chaves de condição
theme	arn:${Partition}:quicksight:${Region}:${Account}:theme/${ResourceId}	aws:ResourceTag/${TagKey}
assignment	arn:${Partition}:quicksight::${Account}:assignment/${ResourceId}	
customization	arn:${Partition}:quicksight:${Region}:${Account}:customization/${ResourceId}	aws:ResourceTag/${TagKey}
namespace	arn:${Partition}:quicksight:${Region}:${Account}:namespace/${ResourceId}	
folder	arn:${Partition}:quicksight:${Region}:${Account}:folder/${ResourceId}	aws:ResourceTag/${TagKey}
emailCustomizationTemplate	arn:${Partition}:quicksight:${Region}:${Account}:email-customization-template/${ResourceId}	
topic	arn:${Partition}:quicksight:${Region}:${Account}:topic/${ResourceId}	aws:ResourceTag/${TagKey}
dashboardSnapshotJob	arn:${Partition}:quicksight:${Region}:${Account}:dashboard/${DashboardId}/snapshot-job/${ResourceId}	aws:ResourceTag/${TagKey}
brand	arn:${Partition}:quicksight:${Region}:${Account}:brand/${ResourceId}	aws:ResourceTag/${TagKey}
custompermissions	arn:${Partition}:quicksight:${Region}:${Account}:custompermissions/${ResourceId}	aws:ResourceTag/${TagKey}

Chaves de condição para a Amazon QuickSight

A Amazon QuickSight define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso por chaves da etiqueta	ArrayOfString
quicksight:AllowedEmbeddingDomains	Filtra o acesso com base nos domínios incorporados permitidos	ArrayOfString
quicksight:DirectoryType	Filtra o acesso pelas opções de gerenciamento de usuários	String
quicksight:Edition	Filtra o acesso pela edição do QuickSight	String
quicksight:Group	Filtra o acesso por ARN QuickSight do grupo	ARN
quicksight:IamArn	Filtra o acesso por usuário IAM ou função ARN	ARN

Chaves de condição	Descrição	Tipo
quicksight:KmsKeyArns	Filtra o acesso por chave KMS ARNs	ArrayOfARN
quicksight:SessionName	Filtra o acesso por nome da sessão	String
quicksight:UserName	Filtra o acesso por nome de usuário	String

Ações, recursos e chaves de condição da API Data do Amazon RDS

A API Data do Amazon RDS (prefixo do serviço: `rds-data`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela API Data do Amazon RDS
- Tipos de recursos definidos pela API Data do Amazon RDS
- Chaves de condição da API Data do Amazon RDS

Ações definidas pela API Data do Amazon RDS

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchExecuteStatement	Concede permissão para executar uma instrução SQL em lote em uma matriz de dados	Write	cluster*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
BeginTransaction	Concede permissão para iniciar uma transação SQL	Gravar	cluster*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
CommitTransaction	Concede permissão para encerrar uma transação SQL iniciada com a BeginTransaction operação e confirma as alterações	Gravar	cluster*		rds-data:BeginTransaction
				aws:ResourceTag/${TagKey} aws:TagKeys	
ExecuteSql	Concede permissão para executar uma ou mais instruções SQL. Esta operação está defasada. Use	Gravar	cluster*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	a ExecuteStatement operação BatchExecuteStatement ou			aws:TagKeys	
ExecuteStatement	Concede permissão para executar uma instrução SQL em um banco de dados	Write	cluster*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
RollbackTransaction	Concede permissão para executar uma reversão de uma transação. Reverter uma transação cancela suas alterações	Write	cluster*		rds-data:BeginTransaction
				aws:ResourceTag/${TagKey} aws:TagKeys	

Tipos de recursos definidos pela API Data do Amazon RDS

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
cluster	`arn:${Partition}:rds:${Region}:${Account}:cluster:${DbClusterInstanceName}`	aws:ResourceTag/${TagKey} aws:TagKeys

Chaves de condição da API Data do Amazon RDS

A API de dados do Amazon RDS define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma IAM política. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves de etiqueta associadas ao recurso	ArrayOfString

Ações, recursos e chaves de condição para autenticação do IAM do Amazon RDS

A autenticação do IAM do Amazon RDS (prefixo do serviço: `rds-db`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela autenticação do IAM do Amazon RDS
- Tipos de recursos definidos pela autenticação do IAM do Amazon RDS
- Chaves de condição para a autenticação do IAM do Amazon RDS

Ações definidas pela autenticação do IAM do Amazon RDS

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de

condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
connect	Permite que a função ou usuário do IAM se conecte ao banco de dados do RDS	Permissions management	db-user*		

Tipos de recursos definidos pela autenticação do IAM do Amazon RDS

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
db-user	`arn:${Partition}:rds-db:${Region}:${Account}:dbuser:${DbiResourceId}/${DbUserName}`	

Chaves de condição para a autenticação do IAM do Amazon RDS

A autenticação do IAM do Amazon RDS não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das instruções da política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o AWS Recycle Bin

AWS A Lixeira (prefixo do serviço:`rbin`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Recycle Bin
- Tipos de recursos definidos pelo AWS Recycle Bin
- Chaves de condição para o AWS Recycle Bin

Ações definidas pelo AWS Recycle Bin

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando

usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateRule	Concede permissão para criar uma regra de recebimento da Lixeira	Gravar	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys rbin:Request/ResourceType	
DeleteRule	Concede permissão para excluir uma regra de retenção de Lixeira	Gravar	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
GetRule	Concede permissão para obter informações detalhadas sobre uma regra de retenção de Lixeira	Leitura	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListRules	Concede permissão para listar as regras de retenção da Lixeira na região	Leitura		rbin:Request/ResourceType	
ListTagsForResource	Concede permissão para listar as etiquetas associadas a um recurso	Leitura	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
LockRule	Concede permissão para bloquear uma regra de retenção de Lixeira existente	Gravar	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
TagResource	Concede permissão para adicionar ou atualizar as etiquetas de um recurso	Tags	rule*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys rbin:Attribute/ResourceType	
UnlockRule	Concede permissão para desbloquear uma regra de retenção de Lixeira existente	Gravar	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
UntagResource	Concede permissão para remover etiquetas associadas a um recurso	Tags	rule*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} aws:TagKeys rbin:Attribute/ResourceType	
UpdateRule	Concede permissão para atualizar uma regra de retenção de Lixeira existente	Gravar	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	

Tipos de recursos definidos pelo AWS Recycle Bin

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
rule	`arn:${Partition}:rbin:${Region}:${Account}:rule/${ResourceName}`	aws:ResourceTag/${TagKey}

Chaves de condição para o AWS Recycle Bin

AWS A Lixeira define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso pela chave e valor de uma etiqueta em uma solicitação	String
aws:ResourceTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta em uma solicitação	ArrayOfString
rbin:Attribute/ResourceType	Filtra o acesso com base no tipo de recurso da regra existente	String
rbin:Request/ResourceType	Filtra o acesso com base no tipo de recurso em uma solicitação	String

Ações, recursos e chaves de condição do Amazon Redshift

O Amazon Redshift (prefixo do serviço: `redshift`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Redshift
- Tipos de recursos definidos pelo Amazon Redshift
- Chaves de condição do Amazon Redshift

Ações definidas pelo Amazon Redshift

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptReservedNodeExchange	Concede permissão para trocar um nó DC1 reservado por um nó DC2 reservado sem alterações na configuração	Gravar			
AddPartner	Concede permissão para adicionar uma integração de parceiros a um cluster	Gravar			
AssociateDataShareConsumer	Concede permissão para associar um consumidor a um compartilhamento de dados	Gravação	datashare*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				redshift:ConsumerArn redshift:AllowWrites	
AuthorizeClusterSecurityGroupIngress	Concede permissão para adicionar uma regra de entrada (ingresso) a um grupo de segurança do Amazon Redshift	Gravar	securitygroup*		
			securitygroupingress-ec2securitygroup*		
AuthorizeDataShare	Concede permissão para autorizar o consumidor de compartilhamento de dados especificado a consumir um compartilhamento de dados	Gerenciamento de permissões	datashare*		
				redshift:ConsumerIdentifier redshift:AllowWrites	
AuthorizeEndpointAccess	Concede permissão para autorizar atividades relacionadas a endpoint para endpoint da vpc gerenciado por redshift	Gerenciamento de permissões			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AuthorizeInboundIntegration [somente permissão]	Concede permissão ao Amazon Redshift para validar continuamente se o data warehouse de destino pode receber dados replicados do ARN de origem	Gravar	integration*		
AuthorizeSnapshotAccess	Concede permissão ao especificado Conta da AWS para restaurar um instantâneo	Gerenciamento de permissões	snapshot*		
BatchDeleteClusterSnapshots	Concede permissão para excluir snapshots em um lote de até 100	Gravação	snapshot*		
BatchModifyClusterSnapshots	Concede permissão para modificar configurações de uma lista de snapshots	Gravação	snapshot*		
CancelQuery [somente permissão]	Concede permissão para cancelar uma consulta por meio do console do Amazon Redshift	Gravação			
CancelQuerySession [somente permissão]	Concede permissão para visualizar consultas no console do Amazon Redshift	Gravação			
CancelResize	Concede permissão para cancelar uma operação de redimensionamento	Gravação	cluster*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CopyClusterSnapshot	Concede permissão para copiar um snapshot de cluster	Gravar	snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAuthenticationProfile	Concede permissão para criar um perfil de autenticação do Amazon Redshift	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateCluster	Concede permissão para criar um cluster.	Gravação	cluster*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterParameterGroup	Concede permissão para criar um grupo de parâmetros do Amazon Redshift	Gravação	parametergroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterSecurityGroup	Concede permissão para criar um grupo de segurança do Amazon Redshift	Gravação	securitygroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterSnapshot	Concede permissão para criar um snapshot manual do cluster especificado	Gravação	snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterSubnetGroup	Concede permissão para criar um grupo de sub-redes do Amazon Redshift	Gravação	subnetgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterUser	Concede permissão para criar automaticamente o usuário especificado do Amazon Redshift se ele não existir	Gerenciamento de permissões	dbuser*		
				redshift:DbUser	
CreateCustomDomainAssociation	Concede permissão para criar um nome de domínio personalizado para um cluster	Gravar	cluster*		acm:DescribeCertificate

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateEndpointAccess	Concede permissão para criar um endpoint da vpc gerenciado por redshift	Gravar			
CreateEventSubscription	Concede permissão para criar uma assinatura de notificação de evento do Amazon Redshift	Gravação	eventsubscription*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateHsmClientCertificate	Concede permissão para criar um certificado de cliente HSM usado por um cluster para se conectar a um HSM	Gravação	hsmclientcertificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateHsmConfiguration	Concede permissão para criar uma configuração do HSM que contém as informações necessárias para um cluster armazenar e usar chaves de criptografia de banco de dados em um módulo de segurança de hardware (HSM)	Gravação	hsmconfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateInboundIntegration [somente permissão]	Concede permissão à entidade principal de origem para criar uma integração de entrada para que os dados sejam replicados da origem para o data warehouse de destino	Gravar			
CreateIntegration	Concede permissão para criar uma integração ETL zero do Amazon Redshift	Gravar	integration*		kms:CreateGrant kms:DescribeKey
				aws:RequestTag/${TagKey} aws:TagKeys redshift:IntegrationSourceArn redshift:IntegrationTargetArn	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateQev2IdcApplication [somente permissão]	Concede permissão para criar uma aplicação idc do qev2	Gravar			sso:CreateApplication sso:PutApplicationAccessScope sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateRedshiftIdcApplication	Concede permissão para criar uma aplicação idc do redshift	Gravar			sso:CreateApplication sso:PutApplicationAccessScope sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant
CreateSavedQuery [somente permissão]	Concede permissão para criar consultas SQL salvas por meio do console do Amazon Redshift	Gravação			
CreateScheduledAction	Concede permissão para criar uma ação programada do Amazon Redshift	Gravar			
CreateSnapshotCopyGrant	Concede permissão para criar uma cópia de instantâneo, conceder e criptografar instantâneos copiados em um destino Região da AWS	Gerenciamento de permissões	snapshotcopygrant*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshotSchedule	Concede permissão para criar uma programação de snapshot	Gravação	snapshotschedule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTags	Concede permissão para adicionar uma ou mais etiquetas a um recurso especificado	Marcação	cluster		
			eventsubscription		
			hsmclientcertificate		
			hsmconfiguration		
			integration		
			parametergroup		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			securitygroup		
			securitygroupingress-cidr		
			securitygroupingress-ec2securitygroup		
			snapshot		
			snapshotcopygrant		
			snapshotschedule		
			subnetgroup		
			usagelimit		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateUsageLimit	Concede permissão para definir um limite de uso.	Gravar	usagelimit*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeauthorizeDataShare	Concede permissão para remover permissão do consumidor da unidade de compartilhamento de dados especificado para consumir uma unidade de compartilhamento de dados	Gerenciamento de permissões	datashare*		
				redshift:ConsumerIdentifier	
DeleteAuthenticationProfile	Concede permissão para excluir um perfil de autenticação do Amazon Redshift	Gravar			
DeleteCluster	Concede permissão para excluir um cluster provisionado anteriormente	Gravação	cluster*		
DeleteClusterParameterGroup	Concede permissão para excluir um grupo de parâmetros do Amazon Redshift	Gravação	parametergroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteClusterSecurityGroup	Concede permissão para excluir um grupo de segurança do Amazon Redshift	Gravação	securitygroup*		
DeleteClusterSnapshot	Concede permissão para excluir um snapshot manual	Gravação	snapshot*		
DeleteClusterSubnetGroup	Concede permissão para excluir um grupo de sub-redes de cluster	Gravar	subnetgroup*		
DeleteCustomDomainAssociation	Concede permissão para excluir um nome de domínio personalizado para um cluster	Gravar	cluster*		
DeleteEndpointAccess	Concede permissão para excluir um endpoint da vpc gerenciado por redshift	Gravar			
DeleteEventSubscription	Concede permissão para excluir uma assinatura de notificação de evento do Amazon Redshift	Gravação	eventsubscription*		
DeleteHsmClientCertificate	Concede permissão para excluir um certificado do cliente HSM	Gravação	hsmclientcertificate*		
DeleteHsmConfiguration	Concede permissão para excluir uma configuração do HSM do Amazon Redshift	Gravar	hsmconfiguration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteIntegration	Concede permissão para excluir uma integração ETL zero do Amazon Redshift	Gravar	integration*		
				aws:ResourceTag/${TagKey}	
DeletePartner	Concede permissão para excluir uma integração de parceiro de um cluster	Gravar			
DeleteQev2IdcApplication [somente permissão]	Concede permissão para excluir uma aplicação idc do qev2	Gravar	qev2idcapplication*		sso:DeleteApplication
DeleteRedshiftIdcApplication	Concede permissão para excluir uma aplicação idc do redshift	Gravar	redshiftidcapplication*		sso:DeleteApplication
DeleteResourcePolicy	Concede permissão para excluir a política de recursos para um recurso especificado	Gerenciamento de permissões	namespace*		
DeleteSavedQueries [somente permissão]	Concede permissão para excluir consultas SQL salvas por meio do console do Amazon Redshift	Gravação			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteScheduledAction	Concede permissão para excluir uma ação programada do Amazon Redshift	Gravação			
DeleteSnapshotCopyGrant	Concede permissão para excluir uma concessão de cópia de snapshot	Gravação	snapshotcopygrant*		
DeleteSnapshotSchedule	Concede permissão para excluir uma programação de snapshot	Gravação	snapshotschedule*		
DeleteTags	Concede permissão para excluir uma etiqueta ou etiquetas de um recurso	Marcação	cluster		
			eventsubscription		
			hsmclientcertificate		
			hsmconfiguration		
			integration		
			parametergroup		
			securitygroup		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			securitygroupingress-cidr		
			securitygroupingress-ec2securitygroup		
			snapshot		
			snapshotcopygrant		
			snapshotschedule		
			subnetgroup		
			usagelimit		
				aws:TagKeys	
DeleteUsageLimit	Concede permissão para excluir um limite de uso.	Gravar	usagelimit*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeregisterNamespace	Concede permissão para cancelar o registro do namespace especificado de um consumidor	Gravar			
DescribeAccountAttributes	Concede permissão para descrever atributos anexados ao especificado Conta da AWS	Leitura			
DescribeAuthenticationProfiles	Concede permissão para descrever perfis de autenticação criados pelo Amazon Redshift	Leitura			
DescribeClusterDbRevisions	Concede permissão para descrever revisões de banco de dados para um cluster	List			
DescribeClusterParameterGroups	Concede permissão para descrever grupos de parâmetros do Amazon Redshift, incluindo os grupo de parâmetros que você criou e o grupo de parâmetros padrão	Leitura			
DescribeClusterParameters	Concede permissão para descrever parâmetros contidos em um grupo de parâmetros do Amazon Redshift	Leitura	parametergroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeClusterSecurityGroups	Concede permissão para descrever grupo de segurança do Amazon Redshift	Leitura			
DescribeClusterSnapshots	Concede permissão para descrever um ou mais objetos do snapshot que contêm metadados sobre seus snapshots de cluster	Leitura			
DescribeClusterSubnetGroups	Concede permissão para descrever um ou mais objetos do grupo de sub-redes do cluster que contêm metadados sobre seus grupos de sub-redes de cluster	Leitura			
DescribeClusterTracks	Concede permissão para descrever os acompanhamentos de manutenção disponíveis	List			
DescribeClusterVersions	Concede permissão para descrever as versões de cluster disponíveis do Amazon Redshift	Leitura			
DescribeClusters	Concede permissão para descrever propriedades de clusters provisionados	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeCustomDomainAssociations	Concede permissão para descrever nomes de domínio personalizados para um cluster	Lista			
DescribeDataShares	Concede permissão para descrever compartilhamento de dados criados e consumidos por seus clusters	Leitura			
DescribeDataSharesForConsumer	Concede permissão para descrever somente compartilhamento de dados consumidos por seus clusters	Leitura			
DescribeDataSharesForProducer	Concede permissão para descrever somente compartilhamento de dados criados por seus clusters	Leitura			
DescribeDefaultClusterParameters	Concede permissão para descrever configurações de parâmetros para uma família de grupos de parâmetros	Leitura			
DescribeEndpointAccess	Concede permissão para descrever endpoints de vpc gerenciados por redshift	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeEndpointAuthorization	Concede permissão para autorizar a descrição da atividade para o endpoint da vpc gerenciado por recursos redshift	Lista			
DescribeEventCategories	Concede permissão para descrever categorias de eventos de todos os tipos de origem de eventos ou de um tipo de origem especificado	Leitura			
DescribeEventSubscriptions	Concede permissão para descrever as assinaturas de notificação de eventos do Amazon Redshift para o especificado Conta da AWS	Leitura			
DescribeEvents	Concede permissão para descrever eventos relacionados aos clusters, grupos de segurança, snapshots e grupos de parâmetros dos últimos 14 dias	List			
DescribeHsmClientCertificates	Concede permissão para descrever certificados do cliente HSM	Leitura			
DescribeHsmConfigurations	Concede permissão para descrever uma configuração do HSM do Amazon Redshift	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeInboundIntegrations	Concede permissão para listar as integrações de entrada	Lista		redshift:InboundIntegrationArn	
DescribeIntegrations	Concede permissão para descrever uma integração ETL zero do Amazon Redshift	Lista	integration*		
				aws:ResourceTag/${TagKey}	
DescribeLoggingStatus	Concede permissão para descrever se as informações, como consultas e tentativas de conexão, estão sendo registradas em log para um cluster	Leitura	cluster*		
DescribeNodeConfigurationOptions	Concede permissão para descrever propriedades de possíveis configurações de nó, como tipo de nó, número de nós e uso de disco para o tipo de ação especificado.	List			
DescribeOrderableClusterOptions	Concede permissão para descrever opções de ordenação de clusters	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribePartners	Concede permissão para recuperar informações sobre as integrações de parceiros definidas para um cluster	Leitura			
DescribeQev2IdcApplications [somente permissão]	Concede permissão para descrever aplicações idc do qev2	Lista			
DescribeQuery [somente permissão]	Concede permissão para descrever uma consulta por meio do console do Amazon Redshift	Leitura			
DescribeRedshiftIdcApplications	Concede permissão para descrever aplicações idc do redshift	Lista			sso:GetApplicationGrant sso:ListApplicationAccessScopes
DescribeReservedNodeExchangeStatus	Concede permissão para descrever detalhes de status de intercâmbio e metadados associados para um intercâmbio de nós reservados. Os status incluem valores como Em andamento e Solicitados	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeReservedNodeOfferings	Concede permissão para descrever ofertas de nós reservados disponíveis pelo Amazon Redshift	Leitura			
DescribeReservedNodes	Concede permissão para descrever os nós reservados	Leitura			
DescribeResize	Concede permissão para descrever a última operação de redimensionamento de um cluster	Leitura	cluster*		
DescribeSavedQueries [somente permissão]	Concede permissão para descrever consultas salvas por meio do console do Amazon Redshift	Leitura			
DescribeScheduledActions	Concede permissão para descrever ações programadas criadas pelo Amazon Redshift	Leitura			
DescribeSnapshotCopyGrants	Concede permissão para descrever concessões de cópia de instantâneo pertencentes ao especificado Conta da AWS no destino Região da AWS	Leitura			
DescribeSnapshotSchedules	Concede permissão para descrever programações de snapshots	Leitura	snapshotschedule*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeStorage	Concede permissão para descrever o tamanho de armazenamento dos backups de nível e o armazenamento provisional	Leitura			
DescribeTable [somente permissão]	Concede permissão para descrever uma tabela por meio do console do Amazon Redshift	Leitura			
DescribeTableRestoreStatus	Concede permissão para descrever o status de uma ou mais solicitações de restauração de tabela feitas usando a ação da RestoreTableFromClusterSnapshot API	Leitura			
DescribeTags	Concede permissão para descrever etiquetas	Leitura	cluster		
			eventsubscription		
			hsmclientcertificate		
			hsmconfiguration		
			integration		
			parametergroup		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			securitygroup		
			securitygroupingress-cidr		
			securitygroupingress-ec2securitygroup		
			snapshot		
			snapshotcopygrant		
			snapshotschedule		
			subnetgroup		
			usagelimit		
DescribeUsageLimits	Concede permissão para descrever limites de uso.	Leitura	usagelimit*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisableLogging	Concede permissão para desabilitar informações de registro em log, como consultas e tentativas de conexão, para um cluster	Gravação	cluster*		
DisableSnapshotCopy	Concede permissão para desabilitar a cópia automática de snapshots para um cluster	Gravação	cluster*		
DisassociateDataShareConsumer	Concede permissão para deassociar um consumidor de um compartilhamento de dados	Gravação	datashare*		
				redshift:ConsumerArn	
EnableLogging	Concede permissão para habilitar informações de registro em log, como consultas e tentativas de conexão, para um cluster	Gravação	cluster*		
EnableSnapshotCopy	Concede permissão para habilitar a cópia automática de snapshots para um cluster	Gravação	cluster*		
ExecuteQuery [somente permissão]	Concede permissão para executar uma consulta por meio do console do Amazon Redshift	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
FailoverPrimaryCompute	Concede permissão para realizar o failover da computação primária de um cluster Multi-AZ para outra AZ	Gravar	cluster*		
FetchResults [somente permissão]	Concede permissão para buscar resultados de consulta por meio do console do Amazon Redshift	Leitura			
GetClusterCredentials	Concede permissão para obter credenciais temporárias para acessar um banco de dados do Amazon Redshift de acordo com o especificado Conta da AWS	Gravar	dbuser*		
			dbname		
				redshift:DbName redshift:DbUser redshift:DurationSeconds	
GetClusterCredentialsWithIAM	Concede permissão para obter credenciais temporárias aprimoradas para acessar um banco de dados do Amazon Redshift de acordo com o especificado Conta da AWS	Gravar	dbname		
				redshift:DbName redshift:DurationSeconds	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetReservedNodeExchangeConfigurationOptions	Concede permissão para obter as opções de configuração para o intercâmbio de nós reservados	Leitura			
GetReservedNodeExchangeOfferings	Concede permissão para obter uma matriz DC2 ReservedNodeOfferings que corresponda ao tipo de pagamento, prazo e preço de uso do determinado nó DC1 reservado	Leitura			
GetResourcePolicy	Concede permissão para obter a política de recursos para um recurso especificado	Leitura	namespace*		
JoinGroup	Concede permissão para juntar os grupos do Amazon Redshift especificados	Permissions management	dbgroup*		
ListDatabases [somente permissão]	Concede permissão para listar bancos de dados por meio do console do Amazon Redshift	Lista			
ListRecommendations	Concede permissão para listar recomendação do Advisor	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListSavedQueries [somente permissão]	Concede permissão para listar consultas salvas por meio do console do Amazon Redshift	List			
ListSchemas [somente permissão]	Concede permissão para listar esquemas por meio do console do Amazon Redshift	List			
ListTables [somente permissão]	Concede permissão para listar tabelas por meio do console do Amazon Redshift	List			
ModifyAquaConfiguration	Concede permissão para modificar a configuração do AQUA de um cluster	Gravar	cluster*		
ModifyAuthenticationProfile	Concede permissão para modificar um perfil de autenticação existente do Amazon Redshift	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ModifyCluster	Concede permissão para modificar as configurações de um cluster	Gravação	cluster*		acm:DescribeCertificate kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					secretsmanager:GetRandomPassword secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
ModifyClusterDbRevision	Concede permissão para modificar a revisão do banco de dados de um cluster	Gravar	cluster*		
ModifyClusterIamRoles	Concede permissão para modificar a lista de funções do AWS Identity and Access Management (IAM) que podem ser usadas por um cluster para acessar outros serviços AWS	Gerenciamento de permissões	cluster*		
ModifyClusterMaintenance	Concede permissão para modificar as configurações de manutenção de um cluster	Gravação			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ModifyClusterParameterGroup	Concede permissão para modificar os parâmetros de um grupo de parâmetros	Gravação	parametergroup*		
ModifyClusterSnapshot	Concede permissão para modificar as configurações de um snapshot	Gravação	snapshot*		
ModifyClusterSnapshotSchedule	Concede permissão para modificar uma programação de snapshot para um cluster	Gravação	cluster*		
ModifyClusterSubnetGroup	Concede permissão para modificar um grupo de sub-redes de cluster de modo a incluir a lista especificada de sub-redes da VPC	Gravar	subnetgroup*		
ModifyCustomDomainAssociation	Concede permissão para modificar um nome de domínio personalizado para um cluster	Gravar	cluster*		acm:DescribeCertificate
ModifyEndpointAccess	Concede permissão para modificar um endpoint da vpc gerenciado por redshift	Gravar			
ModifyEventSubscription	Concede permissão para modificar uma assinatura de notificação de evento existente do Amazon Redshift	Gravar	eventsubscription*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ModifyIntegration	Concede permissão para modificar uma integração ETL zero do Amazon Redshift	Gravar	integration*		
				aws:ResourceTag/${TagKey}	
ModifyQev2IdcApplication [somente permissão]	Concede permissão para modificar uma aplicação idc do qev2	Gravar	qev2idcapplication*		sso:UpdateApplication

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ModifyRedshiftIdcApplication	Concede permissão para modificar uma aplicação idc do redshift	Gravar	redshiftidcapplication*		sso:DeleteApplicationAccessScope sso:DeleteApplicationGrant sso:GetApplicationGrant sso:ListApplicationAccessScopes sso:PutApplicationAccessScope sso:PutApplicationGrant sso:UpdateApplication

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ModifySavedQuery [somente permissão]	Concede permissão para modificar uma consulta salva existente por meio do console do Amazon Redshift	Gravação			
ModifyScheduledAction	Concede permissão para modificar uma ação programada existente do Amazon Redshift	Gravar			
ModifySnapshotCopyRetentionPeriod	Concede permissão para modificar o número de dias para reter os instantâneos no destino Região da AWS após serem copiados da origem Região da AWS	Gravar	cluster*		
ModifySnapshotSchedule	Concede permissão para modificar uma programação de snapshot	Gravação	snapshotschedule*		
ModifyUsageLimit	Concede permissão para modificar um limite de uso.	Gravação	usagelimit*		
PauseCluster	Concede permissão para pausar um cluster	Gravação	cluster*		
PurchaseReservedNodeOffering	Concede permissão para comprar um nó reservado	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutResourcePolicy	Concede permissão para atualizar a política de recursos para um recurso especificado	Gerenciamento de permissões	namespace*		
RebootCluster	Concede permissão para reinicializar um cluster.	Gravar	cluster*		
RegisterNamespace	Concede permissão para registrar o namespace especificado para um consumidor	Gravar			
RejectDataShare	Concede permissão para recusar um datastore compartilhado por outra conta	Permissions management	datashare*		
ResetClusterParameterGroup	Concede permissão para definir um ou mais parâmetros de um grupo de parâmetros como seus valores padrão e definir os valores de origem dos parâmetros como "padrão do mecanismo"	Gravação	parametergroup*		
ResizeCluster	Concede permissão para alterar o tamanho de um cluster	Gravação	cluster*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RestoreFromClusterSnapshot	Concede permissão para criar um cluster de um snapshot	Gravação	cluster*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
			snapshot*		
				aws:TagKeys	
RestoreTableFromClusterSnapshot	Concede permissão para criar uma tabela de uma tabela em um snapshot de cluster do Amazon Redshift	Gravação	cluster*		
			snapshot*		
ResumeCluster	Concede permissão para retomar um cluster.	Gravar	cluster*		
RevokeClusterSecurityGroupIngress	Concede permissão para revogar uma regra de entrada em um grupo de segurança do Amazon Redshift para um intervalo de IP ou grupo de segurança da Amazon previamente autorizado EC2	Gravar	securitygroup*		
			securitygroupingress-ec2securitygroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RevokeEndpointAccess	Concede permissão para revogar o acesso para atividades relacionadas a endpoint para endpoint da vpc gerenciado por redshift	Gerenciamento de permissões			
RevokeSnapshotAccess	Concede permissão para revogar o acesso do especificado Conta da AWS para restaurar um snapshot	Gerenciamento de permissões	snapshot*		
RotateEncryptionKey	Concede permissão para substituir uma chave de criptografia para um cluster	Gravar	cluster*		
UpdatePartnerStatus	Concede permissão para atualizar o status de uma integração de parceiro	Gravar			
ViewQueriesFromConsole [somente permissão]	Concede permissão para visualizar resultados de consulta por meio do console do Amazon Redshift	List			
ViewQueriesInConsole [somente permissão]	Concede permissão para encerrar a execução de consultas e carregamentos por meio do console do Amazon Redshift	List			

Tipos de recursos definidos pelo Amazon Redshift

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
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}	
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 recursos	ARN	Chaves de condição
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}	

Chaves de condição do Amazon Redshift

O Amazon Redshift define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por ações com base no conjunto de valores permitidos para cada uma das etiquetas	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso por ações com base na etiqueta-valor associada ao recurso	String
aws:TagKeys	Filtra o acesso por ações com base na presença de etiquetas obrigatórias na solicitação	ArrayOfString
redshift:AllowWrites	Filtra o acesso pelo parâmetro de entrada allowWrites	Bool
redshift:ConsumerArn	Filtra o acesso pelo ARN do consumidor do compartilhamento de dados	ARN
redshift:ConsumerIdentifier	Filtra o acesso pelo consumidor do compartilhamento de dados	Segmento
redshift:DbName	Filtra o acesso pelo nome do banco de dados	Segmento
redshift:DbUser	Filtra o acesso pelo nome de usuário do banco de dados	Segmento
redshift:DurationSeconds	Filtra o acesso pelo número de segundos até que um conjunto de credenciais temporário expire	String
redshift:InboundIntegrationArn	Filtra o acesso pelo ARN de um recurso de integração ETL zero de entrada	ARN
redshift:IntegrationSourceArn	Filtra o acesso pelo ARN de uma fonte de integração ETL zero	ARN

Chaves de condição	Descrição	Tipo
redshift:IntegrationTargetArn	Filtra o acesso pelo ARN de um destino de integração ETL zero	ARN

Ações, recursos e chaves de condição da API Data do Amazon Redshift

A API Data do Amazon Redshift (prefixo do serviço: `redshift-data`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela DATA API do Amazon Redshift
- Tipos de recursos definidos pela Data API do Amazon Redshift
- Chaves de condição da API Data do Amazon Redshift

Ações definidas pela DATA API do Amazon Redshift

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchExecuteStatement	Concede permissão para executar várias consultas em uma única conexão	Gravar	cluster		
			workgroup		
				redshift-data:sess	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ion-owner-iam-user id redshift-data:glue-catalog-arn	
CancelStatement	Concede permissão para cancelar uma consulta em execução	Write		redshift-data:statement-owner-iam-userid	
DescribeStatement	Concede permissão para recuperar informações detalhadas sobre a execução de uma instrução	Read		redshift-data:statement-owner-iam-userid	
DescribeTable	Concede permissão para recuperar metadados sobre uma tabela específica	Read	cluster*		
			workgroup*		
ExecuteStatement	Concede permissão para executar uma consulta	Gravar	cluster		
			workgroup		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				redshift-data:session-owner-iam-userid redshift-data:glue-catalog-arn	
GetStagingBucketLocation	Concede permissão para obter a localização do bucket de teste para um determinado grupo de trabalho gerenciado	Leitura	managed-workgroup*		
GetStatementResult	Concede permissão para buscar o resultado de uma consulta	Read		redshift-data:statement-owner-iam-userid	
ListDatabases	Concede permissão para listar bancos de dados de um determinado cluster	Read	cluster*		
			workgroup* –		
ListSchemas	Concede permissão para listar esquemas de um determinado cluster	Read	cluster*		
			workgroup* –		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListStatements	Concede permissão para listar consultas de um determinado principal	List		redshift-data:statement-owner-iam-userid	
ListTables	Concede permissão para listar tabelas de um determinado cluster	List	cluster*		
			workgroup*		

Tipos de recursos definidos pela Data API do Amazon Redshift

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
cluster	`arn:${Partition}:redshift:${Region}:${Account}:cluster:${ClusterName}`	aws:ResourceTag/${TagKey}
workgroup	`arn:${Partition}:redshift-serverless:${Region}:${Account}:workgroup/${WorkgroupId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
managed-workgroup	`arn:${Partition}:redshift-serverless:${Region}:${Account}:managed-workgroup/${ManagedWorkgroupId}`	

Chaves de condição da API Data do Amazon Redshift

A API Data do Amazon Redshift define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso pelo valor-etiqueta associado ao recurso	String
redshift-data:glue-catalog-arn	Filtra o acesso por fio de catálogo azul	ARN
redshift-data:session-owner-iam-userid	Filtra o acesso pelo userId do IAM do proprietário da sessão	String
redshift-data:statement-owner-iam-userid	Filtra o acesso pelo proprietário da instrução iam userid	String

Ações, recursos e chaves de condição para o Amazon Redshift Serverless

O Amazon Redshift Serverless (prefixo do serviço: `redshift-serverless`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Redshift Serverless
- Tipos de recursos definidos pelo Amazon Redshift Serverless
- Chaves de condição do Amazon Redshift Serverless

Ações definidas pelo Amazon Redshift Serverless

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar

a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ConvertRecoveryPointToSnapshot	Concede permissão para converter um ponto de recuperação em snapshot	Gravar	recoveryPoint*		
			snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateCustomDomainAssociation	Concede permissão para criar uma associação de domínio personalizado no Amazon Redshift sem servidor	Gravar	workgroup*		acm:DescribeCertificate
CreateEndpointAccess	Concede permissão para criar um endpoint da VPC gerenciado do Amazon Redshift Serverless	Gravar	endpointAccess*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateNamespace	Concede permissão para criar um namespace do Amazon Redshift Serverless	Gravar	namespace*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateReservation	Concede permissão para comprar uma reserva de capacidade de acordo com uma oferta de reserva específica, para um número específico de RPUs	Gravar			
CreateScheduledAction	Concede permissão para criar uma ação programada para um namespace especificado do Amazon Redshift sem servidor	Gravar	namespace*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSnapshot	Concede permissão para criar um snapshot de todos os bancos de dados em um namespace	Gravar	snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshotCopyConfiguration	Concede permissão para criar uma configuração de cópia de snapshot para um namespace especificado do Amazon Redshift sem servidor	Gravar	namespace*		
CreateUsageLimit	Concede permissão para criar um limite de uso para um tipo de uso especificado do Amazon Redshift Serverless	Gravar			
CreateWorkgroup	Concede permissão para criar um grupo de trabalho do Amazon Redshift Serverless	Gravar	workgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCustomDomainAssociation	Concede permissão para excluir uma associação de domínio personalizado	Gravar	workgroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteEndpointAccess	Concede permissão para excluir um endpoint da VPC gerenciado do Amazon Redshift Serverless	Gravar	endpointAccess*		
DeleteNamespace	Concede permissão para excluir um namespace do Amazon Redshift Serverless	Gravar	namespace*		kms:DescribeKey kms:RetireGrant secretsmanager:DeleteSecret secretsmanager:DescribeSecret
DeleteResourcePolicy	Concede permissão para excluir a política de recurso especificada	Gravar			
DeleteScheduledAction	Concede permissão para excluir uma ação programada do Amazon Redshift sem servidor	Gravar			
DeleteSnapshot	Concede permissão para excluir um snapshot do Amazon Redshift Serverless	Gravar	snapshot*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteSnapshotCopyConfiguration	Concede permissão para excluir uma configuração de cópia de snapshot para um namespace do Amazon Redshift sem servidor	Gravar			
DeleteUsageLimit	Concede permissão para excluir um limite de uso do Amazon Redshift Serverless	Gravar			
DeleteWorkgroup	Concede permissão para excluir um grupo de trabalho	Gravar	workgroup *		
DescribeOneTimeCredit [somente permissão]	Concede permissão para ver no console do Amazon Redshift sem servidor o número restante de créditos de avaliação gratuita e sua data de expiração	Leitura			
GetCredentials	Concede permissão para obter um nome de usuário e senha temporária do banco de dados com autorização temporária para fazer logon no Amazon Redshift Serverless	Gravar	workgroup *		
GetCustomDomainAssociation	Concede permissão para obter informações sobre uma associação de domínio personalizado específica	Leitura	workgroup *		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetEndpointAccess	Concede permissão para criar um endpoint da VPC gerenciado do Amazon Redshift Serverless	Leitura	endpointAccess*		
GetManagedWorkgroup	Concede permissão para criar um grupo de trabalho Amazon Redshift Managed Serverless com as definições de configuração especificadas	Leitura	managed-workgroup*		
GetNamespace	Concede permissão para obter informações sobre um namespace no Amazon Redshift Serverless	Leitura	namespace*		
GetRecoveryPoint	Concede permissão para obter informações sobre um ponto de recuperação	Leitura	recoveryPoint*		
GetReservation	Concede permissão para obter um objeto de reserva específico	Leitura			
GetReservationOffering	Concede permissão para obter uma oferta de reserva específica	Leitura			
GetResourcePolicy	Concede permissão para obter uma política de recurso	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetScheduledAction	Concede permissão para obter informações sobre uma ação programada específica	Leitura			
GetSnapshot	Concede permissão para obter informações sobre um snapshot específico	Leitura	snapshot*		
GetTableRestoreStatus	Concede permissão para obter o status de restauração da tabela sobre um snapshot específico	Leitura			
GetTrack	Concede permissão para obter informações sobre uma faixa no Amazon Redshift Serverless	Leitura			
GetUsageLimit	Concede permissão para obter informações sobre um limite de uso no Amazon Redshift Serverless	Leitura			
GetWorkgroup	Concede permissão para obter informações sobre um grupo de trabalho específico	Leitura	workgroup*		
ListCustomDomainAssociations	Concede permissão para listar associações de domínios personalizados no Amazon Redshift sem servidor	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListEndpointAccess	Concede permissão para listar EndpointAccess objetos e informações relevantes	Lista	endpointAccess*		
ListManagedWorkgroups	Concede permissão para listar grupos de trabalho gerenciados no Amazon Redshift Serverless	Lista			
ListNamespaces	Concede permissão para listar um namespace no Amazon Redshift Serverless	Lista			
ListRecoveryPoints	Concede permissão para listar qualquer matriz de pontos de recuperação	Lista	namespace		
ListReservationOfferings	Concede permissão para listar todas as ofertas de reserva de capacidade disponíveis	Lista			
ListReservations	Concede permissão para listar todas as reservas	Lista			
ListScheduledActions	Concede permissão para listar ações programadas	Lista			
ListSnapshotCopyConfigurations	Concede permissão para listar SnapshotCopyConfiguration objetos e informações relevantes	Lista	namespace		
ListSnapshots	Concede permissão para listar snapshots	Lista	snapshot*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTableRestoreStatus	Concede permissão para listar o status de restauração da tabela	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas atribuídas a um recurso	Lista	namespace		
			workgroup		
				aws:ResourceTag/${TagKey}	
ListTracks	Concede permissão para listar faixas disponíveis no Amazon Redshift Serverless	Lista			
ListUsageLimits	Concede permissão para listar todos os limites de uso no Amazon Redshift Serverless	Lista			
ListWorkgroups	Concede permissão para listar grupos de trabalho no Amazon Redshift Serverless	Lista			
PutResourcePolicy	Concede permissão para criar ou atualizar uma política de recurso	Gravar			
RestoreFromRecoveryPoint	Concede permissão para restaurar os dados de um ponto de recuperação	Gravar	recoveryPoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RestoreFromSnapshot	Concede permissão para restaurar um namespace de um snapshot	Gravar	snapshot*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
RestoreTableFromRecoveryPoint	Concede permissão para restaurar uma tabela de um ponto de recuperação	Gravar	namespace*		
			recoveryPoint*		
RestoreTableFromSnapshot	Concede permissão para restaurar uma tabela de um snapshot	Gravar	namespace*		
			snapshot*		
TagResource	Concede permissão para atribuir uma ou mais etiquetas a um recurso	Tags	namespace		
			recoveryPoint		
			snapshot		
			workgroup		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permissão para remover um etiqueta ou um conjunto de etiquetas de um recurso	Tags	namespace		
			recoveryPoint		
			snapshot		
			workgroup		
				aws:TagKeys	
UpdateCustomDomainAssociation	Concede permissão para atualizar um certificado associado a um domínio personalizado	Gravar	workgroup*		acm:DescribeCertificate
UpdateEndpointAccess	Concede permissão para atualizar um endpoint da VPC gerenciado do Amazon Redshift Serverless	Gravar	endpointAccess*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateNamespace	Concede permissão para atualizar um namespace com as definições de configuração especificadas	Gravar	namespace*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
UpdateScheduledAction	Concede permissão para atualizar uma ação programada	Gravar			
UpdateSnapshot	Concede permissão para atualizar um snapshot	Gravar	snapshot*		
UpdateSnapshotCopyConfiguration	Concede permissão para atualizar uma configuração de cópia de snapshot para um namespace do Amazon Redshift sem servidor	Gravar			
UpdateUsageLimit	Concede permissão para atualizar um limite de uso no Amazon Redshift Serverless	Gravar			
UpdateWorkgroup	Concede permissão para atualizar um grupo de trabalho do Amazon Redshift Serverless com as definições de configuração especificadas	Gravar	workgroup*		

Tipos de recursos definidos pelo Amazon Redshift Serverless

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}`	

Chaves de condição do Amazon Redshift Serverless

O Amazon Redshift Serverless define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString
redshift-serverless:endpointAccessId	Filtra o acesso pelo identificador de acesso do endpoint	String
redshift-serverless:managedWorkgroupName	Filtra o acesso pelo identificador do grupo de trabalho gerenciado	String
redshift-serverless:namespaceId	Filtra o acesso pelo identificador do namespace	String
redshift-serverles	Filtra o acesso pelo identificador de ponto de recuperação	String

Chaves de condição	Descrição	Tipo
s:recoveryPointId		
redshift-serverless:snapshotId	Filtra o acesso pelo identificador do snapshot	String
redshift-serverless:tableRestoreRequestId	Filtra o acesso pelo identificador de solicitação de restauração da tabela	String
redshift-serverless:workgroupId	Filtra o acesso pelo identificador do grupo de trabalho	String

Ações, recursos e chaves de condição do Amazon Rekognition

O Amazon Rekognition (prefixo do serviço: `rekognition`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Rekognition
- Tipos de recursos definidos pelo Amazon Rekognition
- Chaves de condição do Amazon Rekognition

Ações definidas pelo Amazon Rekognition

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateFaces	Concede permissão para associar várias faces individuais a um único usuário	Gravar	collection*		
CompareFaces	Concede permissão para comparar faces na imagem de origem de entrada com cada face detectada na imagem de entrada de destino	Leitura			
CopyProjectVersion	Concede permissão para copiar uma versão de modelo existente para uma nova versão do modelo	Gravar	project*		
			projectversion*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCollection	Concede permissão para criar uma coleção em um Região da AWS	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataset	Concede permissão para criar um conjunto de dados do	Gravar	project*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	Amazon Rekognition Custom Labels			aws:RequestTag/${TagKey} aws:TagKeys	
CreateFaceLivenessSession	Concede permissão para criar uma sessão de prova de vida ativa	Gravar			
CreateProject	Concede permissão para criar um projeto do Amazon Rekognition Custom Labels	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProjectVersion	Concede permissão para começar a treinar uma versão de um modelo	Gravar	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStreamProcessor	Concede permissão para criar um processador de transmissão do Amazon Rekognition	Gravar	collection*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUser	Concede permissão para criar um novo usuário em uma coleção usando o ID de usuário exclusivo fornecido	Gravar	collection*		
DeleteCollection	Concede permissão para excluir a coleção especificada	Gravar	collection*		
DeleteDataset	Concede permissão para excluir um conjunto de dados de rótulos personalizados do Amazon Rekognition Custom Labels	Gravar	dataset*		
DeleteFaces	Concede permissão para excluir faces de uma coleção	Gravar	collection*		
DeleteProject	Concede permissão para excluir um projeto	Gravar	project*		
DeleteProjectPolicy	Concede permissão para excluir uma política de recursos anexada a um projeto	Gravar	project*		
DeleteProjectVersion	Concede permissão para excluir um modelo	Gravar	projectversion*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteStreamProcessor	Concede permissão para excluir o processador de transmissão especificado	Gravar	streamprocessor*		
DeleteUser	Concede permissão para excluir um usuário de uma coleção com base no ID do usuário fornecido	Gravar	collection*		
DescribeCollection	Concede permissão para ler detalhes sobre uma coleção	Leitura	collection*		
DescribeDataset	Concede permissão para descrever um conjunto de dados do Amazon Rekognition Custom Labels	Leitura	dataset*		
DescribeProjectVersions	Concede permissão para listar as versões de um modelo em um projeto do Amazon Rekognition Custom Labels	Leitura	project*		
DescribeProjects	Concede permissão para listar projetos do Amazon Rekognition Custom Labels	Leitura			
DescribeStreamProcessor	Concede permissão para obter informações sobre o processador de transmissão especificado	Leitura	streamprocessor*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DetectCustomLabels	Concede permissão para detectar rótulos personalizados em uma imagem fornecida	Leitura	projectversion*		
DetectFaces	Concede permissão para detectar faces humanas em uma imagem fornecida como entrada	Leitura			
DetectLabels	Concede permissão para detectar instâncias de rótulos de mundo real em uma imagem fornecida como entrada	Leitura			
DetectModerationLabels	Concede permissão para detectar rótulos de moderação dentro da imagem de entrada	Leitura	projectversion		
DetectProtectiveEquipment	Concede permissão para detectar equipamentos de proteção individual na imagem de entrada	Leitura			
DetectText	Concede permissão para detectar texto na imagem de entrada e converte-lo em texto legível por máquina	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateFaces	Concede permissão para remover a associação entre um ID de usuário e um ID facial	Gravar	collection*		
DistributeDatasetEntries	Concede permissão para distribuir as entradas em um conjunto de dados de treinamento no conjunto de dados de treinamento e no conjunto de dados de teste de um projeto	Gravar	dataset*		
GetCelebrityInfo	Concede permissão para ler o nome e informações adicionais de uma celebridade	Leitura			
GetCelebrityRecognition	Concede permissão para ler os resultados de reconhecimento de celebridades encontrados em um vídeo armazenado por um trabalho assíncrono de reconhecimento de celebridades	Leitura			
GetContentModeration	Concede permissão para ler os resultados da análise de moderação de conteúdo encontrados em um vídeo armazenado por um trabalho de moderação de conteúdo assíncrono	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetFaceDetection	Concede permissão para ler os resultados da detecção de faces encontrados em um vídeo armazenado por um trabalho de detecção de rosto assíncrono	Leitura			
GetFaceLivenessSessionResults	Concede permissão para obter os resultados de uma sessão de prova de vida ativa	Leitura			
GetFaceSearch	Concede permissão para ler as faces de coleção correspondentes encontradas em um vídeo armazenado por um trabalho de pesquisa facial assíncrona	Leitura			
GetLabelDetection	Concede permissão para ler os resultados detectados da etiqueta encontrados em um vídeo armazenado por um trabalho assíncrono de detecção de etiquetas	Leitura			
GetMediaAnalysisJob	Concede permissão para ler a referência aos resultados do trabalho no S3 e informações adicionais sobre um trabalho de análise de mídia	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetPersonTracking	Concede permissão para ler a lista de pessoas detectadas em um vídeo armazenado por um trabalho de rastreamento de pessoa assíncrona	Leitura			
GetSegmentDetection	Concede permissão para obter os segmentos de vídeo encontrados em um vídeo armazenado por um trabalho de detecção de segmento assíncrono	Leitura			
GetTextDetection	Concede permissão para obter o texto encontrado em um vídeo armazenado por um trabalho de detecção de texto assíncrono	Leitura			
IndexFaces	Concede permissão para atualizar uma coleção existente com faces detectadas na imagem de entrada	Gravar	collection*		
ListCollections	Concede permissão para ler os IDs de coleta em sua conta	Leitura			
ListDatasetEntries	Concede permissão para listar as entradas do conjunto de dados em um conjunto de dados de rótulos personalizados do Amazon Rekognition Custom Labels existente	Leitura	dataset*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDatasetLabels	Concede permissão para listar os rótulos em um conjunto de dados	Leitura	dataset*		
ListFaces	Concede permissão para ler metadados para rostos na coleção específica	Leitura	collection*		
ListMediaAnalysisJobs	Concede permissão para ler a lista de trabalhos de análise de mídia	Leitura			
ListProjectPolicies	Concede permissão para listar as políticas de recursos anexadas a um projeto	Leitura	project*		
ListStreamProcessors	Concede permissão para obter uma lista dos processadores de transmissão	Lista			
ListTagsForResource	Concede permissão para retornar uma lista de etiquetas associadas a um recurso	Leitura	collection		
			dataset		
			project		
			projectversion		
			streamprocessor		
ListUsers	Concede permissão para listar UserIds e UserStatus	Leitura	collection*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutProjectPolicy	Concede permissão para anexar uma política de recursos a um projeto	Gravar	project*		
RecognizeCelebrities	Concede permissão para detectar celebridades na imagem de entrada	Leitura			
SearchFaces	Concede permissão para pesquisar a coleção especificada para o ID facial fornecido	Leitura	collection*		
SearchFacesByImage	Concede permissão para pesquisar a coleção especificada para a maior face na imagem de entrada	Leitura	collection*		
SearchUsers	Concede permissão para pesquisar a coleção especificada para obter um resultado correspondente ao usuário com determinada ID facial ou ID de usuário	Leitura	collection*		
SearchUsersByImage	Concede permissão para pesquisar a coleção especificada para obter um resultado correspondente ao usuário usando a maior face na imagem de entrada	Leitura	collection*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartCelebrityRecognition	Concede permissão para iniciar o reconhecimento assíncrono de celebridades em um vídeo armazenado	Gravar			
StartContentModeration	Concede permissão para iniciar a detecção assíncrona de conteúdo adulto explícito ou sugestivo em um vídeo	Gravar			
StartFaceDetection	Concede permissão para iniciar a detecção assíncrona de faces em um vídeo armazenado	Gravar			
StartFaceLivenessSession	Concede permissão para iniciar a transmissão de vídeo para uma sessão de prova de vida ativa	Gravar			
StartFaceSearch	Concede permissão para iniciar a pesquisa assíncrona de faces em uma coleção que correspondem às faces de pessoas detectadas em um vídeo	Gravar	collection*		
StartLabelDetection	Concede permissão para iniciar a detecção assíncrona de rótulos em um vídeo armazenado	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartMediaAnalysisJob	Concede permissão para iniciar um trabalho de análise de mídia	Gravar	projectversion		
StartPersonTracking	Concede permissão para iniciar o rastreamento assíncrono de pessoas em um vídeo armazenado	Gravar			
StartProjectVersion	Concede permissão para iniciar a execução de uma versão de modelo	Gravar	projectversion*		
StartSegmentDetection	Concede permissão para iniciar a detecção assíncrona de segmentos em um vídeo armazenado	Gravar			
StartStreamProcessor	Concede permissão para iniciar a execução de um processador de stream	Gravar	streamprocessor*		
StartTextDetection	Concede permissão para iniciar a detecção assíncrona de texto em um vídeo armazenado	Gravar			
StopProjectVersion	Concede permissão para interromper uma versão de modelo em execução	Gravar	projectversion*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopStreamProcessor	Concede permissão para interromper um processador de stream em execução	Gravar	streamprocessor*		
TagResource	Concede permissão para adicionar uma ou mais etiquetas a um recurso	Marcação	collection		
			dataset		
			project		
			projectversion		
			streamprocessor		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover uma ou mais etiquetas de um recurso	Tags	collection		
			dataset		
			project		
			projectversion		
			streamprocessor		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
UpdateDatasetEntries	Concede permissão para adicionar ou atualizar uma ou mais linhas JSON (entradas) em um conjunto de dados	Gravar	dataset*		
UpdateStreamProcessor	Concede permissão para modificar propriedades de um processador de fluxo	Gravar	streamprocessor*		

Tipos de recursos definidos pelo Amazon Rekognition

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
collection	`arn:${Partition}:rekognition:${Region}:${Account}:collection/${CollectionId}`	aws:ResourceTag/${TagKey}
streamprocessor	`arn:${Partition}:rekognition:${Region}:${Account}:streamprocessor/${StreamprocessorId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
project	`arn:${Partition}:rekognition:${Region}:${Account}:project/${ProjectName}/${CreationTimestamp}`	aws:ResourceTag/${TagKey}
projectversion	`arn:${Partition}:rekognition:${Region}:${Account}:project/${ProjectName}/version/${VersionName}/${CreationTimestamp}`	aws:ResourceTag/${TagKey}
dataset	`arn:${Partition}:rekognition:${Region}:${Account}:project/${ProjectName}/dataset/${DatasetType}/${CreationTimestamp}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Rekognition

O Amazon Rekognition define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	String

Chaves de condição	Descrição	Tipo
aws:TagKeys	Filtra o acesso pelas chaves de etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS RePost Private

AWS O RePost Private (prefixo do serviço:`repostspace`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS RePost Private
- Tipos de recursos definidos pelo AWS RePost Private
- Chaves de condição para AWS RePost Private

Ações definidas pelo AWS RePost Private

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchAddChannelRoleToAccessors	Concede permissão para adicionar uma função a usuários e grupos em um canal re:post privado em sua conta	Gravar	space*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchAddRole	Concede permissão para adicionar uma função a usuários e grupos em um re:post privado em sua conta	Gravar	space*		
BatchRemoveChannelRoleFromAccessors	Concede permissão para remover uma função de usuários e grupos em um canal re:post privado em sua conta	Gravar	space*		
BatchRemoveRole	Concede permissão para remover uma função de usuários e grupos em um re:post privado em sua conta	Gravar	space*		
CreateChannel	Concede permissão para criar um novo canal privado Re:post em sua conta	Gravar	space*		
CreateSpace	Concede permissão para criar um novo re:Post privado em sua conta	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteSpace	Concede permissão para excluir um re:Post privado da sua conta	Gravar	space*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeregisterAdmin	Concede permissão para remover um administrador de um re:Post privado em sua conta	Gravar	space*		
GetChannel	Concede permissão para obter a descrição de um canal em privado Re:post em sua conta	Leitura	space*		
GetSpace	Concede permissão para obter a descrição de um re:Post privado em sua conta	Leitura	space*		
ListChannels	Concede permissão para listar todos os canais em um re:post privado em sua conta	Leitura	space*		
ListSpaces	Concede permissão para listar todos os re:Post privados em sua conta	Leitura			
ListTagsForResource	Concede permissão para listar as etiquetas associadas a um recurso	Leitura	space*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RegisterAdmin	Concede permissão para adicionar um administrador a um re:post privado em sua conta	Gravar	space*		
SendInvites	Concede permissão para enviar convites para usuários de um re:Post privado em sua conta	Gravar	space*		
TagResource	Concede permissão para marcar um recurso	Marcação	space*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para desmarcar um recurso	Tags	space*		
				aws:TagKeys	
UpdateChannel	Concede permissão para atualizar um canal em privado re:Post em sua conta	Gravar	space*		
UpdateSpace	Concede permissão para atualizar um re:Post privado em sua conta	Gravar	space*		

Tipos de recursos definidos pelo AWS RePost Private

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
space	`arn:${Partition}:repostspace:${Region}:${Account}:space/${ResourceId}`	aws:ResourceTag/${TagKey}

Chaves de condição para AWS RePost Private

AWS O RePost Private define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS Resilience Hub

AWS O Resilience Hub (prefixo do serviço:`resiliencehub`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Resilience Hub
- Tipos de recursos definidos pelo AWS Resilience Hub
- Chaves de condição do AWS Resilience Hub

Ações definidas pelo AWS Resilience Hub

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptResourceGroupingRecommendations	Concede permissão para aceitar recomendações de agrupamento de recursos	Gravar	application*		
AddDraftAppVersionResourceMappings	Concede permissão para adicionar mapeamentos de recursos de versão da aplicação de rascunho	Gravar	application*		cloudformation:DescribeStacks cloudformation:Lis

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					tStackResources resource-groups:GetGroup resource-groups:ListGroupResources servicecatalog:GetApplication servicecatalog:ListAssociatedResources
BatchUpdateRecommendationStatus	Concede permissão para incluir ou excluir uma ou mais recomendações operacionais	Gravar	application*		
CreateApp	Concede permissão para criar aplicação	Gravar	application*		iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAppVersionAppComponent	Concede permissão para criar componentes de uma aplicação	Gravar	application*		
CreateAppVersionResource	Concede permissão para criar recursos de uma aplicação	Gravar	application*		
CreateRecommendationTemplate	Concede permissão para criar um modelo de recomendação	Gravar	application*		s3:CreateBucket s3:ListBucket s3:PutObject
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateResiliencyPolicy	Concede permissão para criar uma política de resiliência	Gravar	resiliency-policy*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApp	Concede permissão para excluir aplicação em lote	Gravar	application*		
DeleteAppAssessment	Concede permissão para excluir avaliação de aplicação em lote	Gravar	application*		
DeleteAppInputSource	Concede permissão para remover a fonte de entrada da aplicação	Gravar	application*		
DeleteAppVersionAppComponent	Concede permissão para excluir componentes de uma aplicação	Gravar	application*		
DeleteAppVersionResource	Concede permissão para excluir recursos de uma aplicação	Gravar	application*		
DeleteRecommendationTemplate	Concede permissão para excluir um modelo de recomendação em lote	Gravar	application*		
DeleteResiliencyPolicy	Concede permissão para excluir uma política de resiliência em lote	Gravar	resiliency-policy*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeApp	Concede permissão para descrever aplicação	Leitura	application*		
DescribeAppAssessment	Concede permissão para descrever avaliação de aplicação	Leitura	application*		
DescribeAppVersion	Concede permissão para descrever a versão de uma aplicação	Leitura	application*		
DescribeAppVersionAppComponent	Concede permissão para descrever o componente de app da versão de uma aplicação	Leitura	application*		
DescribeAppVersionResource	Concede permissão para descrever o recurso de uma versão de uma aplicação	Leitura	application*		
DescribeAppVersionResourcesResolutionStatus	Concede permissão para descrever resolução de aplicação	Leitura	application*		
DescribeAppVersionTemplate	Concede permissão para descrever um modelo de versão de aplicação	Leitura	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeDraftAppVersionResourcesImportStatus	Concede permissão para descrever o status de importação de recursos de versão da aplicação de rascunho	Leitura	application*		
DescribeMetricsExport	Concede permissão para descrever a exportação de métricas	Leitura			
DescribeResiliencyPolicy	Concede permissão para descrever política de resiliência	Leitura	resiliency-policy*		
DescribeResourceGroupingRecommendationTask	Concede permissão para descrever o status mais recente do processo de recomendação de agrupamento	Leitura	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ImportResourcesToDraftAppVersion	Concede permissão para importar recursos de versão da aplicação de rascunho	Gravar	application*		cloudformation:DescribeStacks cloudformation:ListStackResources resource-groups:GetGroup resource-groups:ListGroupResources servicecatalog:GetApplication servicecatalog:ListAssociatedResources
ListAlarmRecommendations	Concede permissão para listar recomendação de alarme	Lista	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAppAssessmentComplianceDrifts	Concede permissão para listar desvios de conformidade que foram detectados durante a execução de uma avaliação	Lista	application*		
ListAppAssessmentResourceDrifts	Concede permissão para listar desvios de recurso que foram detectados durante a execução de uma avaliação	Lista	application*		
ListAppAssessments	Concede permissão para listar avaliação de aplicação	Lista			
ListAppComponentCompliances	Concede permissão para listar conformidades dos componentes de uma aplicação	Lista	application*		
ListAppComponentRecommendations	Concede permissão para listar recomendações de componentes de aplicações	Lista	application*		
ListAppInputSources	Concede permissão para listar as fontes de entrada da aplicação	Lista	application*		
ListAppVersionAppComponents	Concede permissão para listar componentes de app da versão de uma aplicação	Lista	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAppVersionResourceMappings	Concede permissão para mapeamentos de recursos de versão da aplicação	Lista	application*		
ListAppVersionResources	Concede permissão para listar os recursos da aplicação	Lista	application*		
ListAppVersions	Concede permissão para listar versão da aplicação	Lista	application*		
ListApps	Concede permissão para listar aplicações	Lista			
ListMetrics	Concede permissão para listar métricas	Lista			
ListRecommendationTemplates	Concede permissão para listar modelos de recomendação	Lista	application*		
ListResiliencyPolicies	Concede permissão para listar suas políticas de resiliência	Lista			
ListResourceGroupingRecommendations	Concede permissão para listar recomendações de agrupamento de recursos	Lista	application*		
ListSopRecommendations	Concede permissão para listar recomendação de SOP	Lista	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListSuggestedResiliencyPolicies	Concede permissão para listar suas políticas de resiliência sugeridas	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura			
ListTestRecommendations	Concede permissão para listar recomendações de teste	Lista	application*		
ListUnsupportedAppVersionResources	Concede permissão para listar recursos de versão de aplicações sem suporte	Lista	application*		
PublishAppVersion	Concede permissão para publicar versão da aplicação	Gravar	application*		
PutDraftAppVersionTemplate	Concede permissão para colocar um modelo de versão da aplicação	Gravar	application*		
RejectResourceGroupingRecommendations	Concede permissão para rejeitar recomendações de agrupamento de recursos	Gravar	application*		
RemoveDraftAppVersionResourceMappings	Concede permissão para remover mapeamentos de recursos de aplicação de rascunho	Gravar	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ResolveAppVersionResources	Concede permissão para resolver recursos de versão da aplicação	Gravar	application*		cloudformation:DescribeStacks cloudformation:ListStackResources resource-groups:GetGroup resource-groups:ListGroupResources servicecatalog:GetApplication servicecatalog:ListAssociatedResources

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartAppAssessment	Concede permissão para criar avaliação de aplicação	Gravar	application*		cloudformation:DescribeStacks cloudformation:ListStackResources cloudwatch:DescribeAlarms cloudwatch:GetMetricData cloudwatch:GetMetricStatistics cloudwatch:PutMetricData ec2:DescribeRegions fis:GetExperimentTemplate

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					fis:ListExperimentTemplates fis:ListExperiments resource-groups:GetGroup resource-groups:ListGroupResources servicecatalog:GetApplication servicecatalog:ListAssociatedResources ssm:GetParametersByPath

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
StartMetricsExport	Concede permissão para iniciar a exportação de métricas	Gravar			
StartResourceGroupingRecommendationTask	Concede permissão para iniciar o processo de geração de recomendações de agrupamento	Gravar	application*		
TagResource	Concede permissão para atribuir uma tag de recurso	Tags	app-assessment		
			application		
			recommendation-template		
			resiliency-policy		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso	Tags	app-assessment		
			application		
			recommendation-template		
			resiliency-policy		
				aws:TagKeys	
UpdateApp	Concede permissão para atualizar aplicação	Gravar	application*		iam:PassRole
UpdateAppVersion	Concede permissão para atualizar a versão da aplicação	Gravar	application*		
UpdateAppVersionAppComponent	Concede permissão para excluir componentes de app de uma aplicação	Gravar	application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateAppVersionResource	Concede permissão para atualizar o recurso de uma aplicação	Gravar	application*		
UpdateResiliencyPolicy	Concede permissão para atualizar política de resiliência	Gravar	resiliency-policy*		

Tipos de recursos definidos pelo AWS Resilience Hub

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
recommendation-template	`arn:${Partition}:resiliencehub:${Region}:${Account}:recommendation-template/${RecommendationTemplateId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Resilience Hub

AWS O Resilience Hub define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Resource Access Manager (RAM)

AWS O Resource Access Manager (RAM) (prefixo do serviço:`ram`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Resource Access Manager (RAM)
- Tipos de recursos definidos pelo AWS Resource Access Manager (RAM)
- Chaves de condição do AWS Resource Access Manager (RAM)

Ações definidas pelo AWS Resource Access Manager (RAM)

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptResourceShareInvitation	Concede permissão para aceitar o convite de compartilhamento de recursos especificado	Gravar	resource-share-invitation*		
				ram:ShareOwnerAccountId ram:ResourceShareName	
AssociateResourceShare	Concede permissão para associar o (s) and/or principal (s) do (s) recurso (s) a um compartilhamento de recursos	Gravar	resource-share*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals ram:Principal ram:RequestedResourceType ram:ResourceArn	
AssociateResourceSharePermission	Concede permissão para associar uma permissão a um compartilhamento de recursos	Gravar	customer-managed-permission*		
			permission*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			resource-share*		
CreatePermission	Concede permissão para criar uma permissão que pode ser associada a um compartilhamento de recursos	Gravar		ram:PermissionArn ram:PermissionResourceType aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	ram:TagResource
CreatePermissionVersion	Concede permissão para criar uma nova versão de uma permissão que pode ser associada a um compartilhamento de recursos	Gravar	customer-managed-permission*		
				ram:PermissionArn ram:PermissionResourceType	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateResourceShare	Concede permissão para criar um compartilhamento de recursos com o (s) and/or principal (s) do (s) recurso (s) fornecido (s)	Gravar		aws:RequestTag/${TagKey} aws:TagKeys ram:RequestedResourceType ram:ResourceArn ram:RequestedAllowsExternalPrincipals ram:Principal ram:AllowsExternalPrincipals	
DeletePermission	Concede permissão para excluir uma permissão especificada	Gravar	customer-managed-permission *		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} ram:PermissionArn ram:PermissionResourceType	
DeletePermissionVersion	Concede permissão para excluir uma versão especificada de uma permissão	Gravar	customer-managed-permission*		
				ram:PermissionArn ram:PermissionResourceType	
DeleteResourceShare	Concede permissão para excluir um compartilhamento de recursos	Gravar	resource-share*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals	
DisassociateResourceShare	Concede permissão para desassociar o (s) and/or principal (s) do (s) recurso (s) de um compartilhamento de recursos	Gravar	resource-share*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals ram:Principal ram:RequestedResourceType ram:ResourceArn	
DisassociateResourceSharePermission	Concede permissão para desassociar uma permissão de um compartilhamento de recursos	Write	customer-managed-permission*		
			permission*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			resource-share*		
EnableSharingWithAwsOrganization	Concede permissão para acessar uma organização do cliente e criar uma SLR na conta do cliente.	Gerenciamento de permissões			iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:EnableAWSServiceAccess
GetPermission	Concede permissão para obter o conteúdo de uma permissão de AWS RAM	Leitura	customer-managed-permission*		
			permission*		
				ram:PermissionArn	
GetResourcePolicies	Concede permissão para obter as políticas para os recursos especificados que você possui e compartilhou	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetResourceShareAssociations	Concede permissão para obter um conjunto de associações de uma lista fornecida ou com um status do tipo especificado	Read			
GetResourceShareInvitations	Concede permissão para obter convites para compartilhamento de recursos pelo ARN do convite especificado ou por aqueles do compartilhamento de recursos	Read			
GetResourceShares	Concede permissão para obter um conjunto de compartilhamentos de recursos de uma lista fornecida ou com um status especificado	Read		aws:RequestTag/${TagKey} aws:TagKeys	
ListPendingInvitationResources	Concede permissão para listar os recursos em um compartilhamento de recursos que são compartilhados com você, mas para os quais o convite ainda está pendente	Leitura	resource-share-invitation*		
				ram:ResourceShareName	
ListPermissionAssociations	Concede permissão para listar informações sobre a permissão e quaisquer associações	Lista	customer-managed-permission*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			permission*		
				ram:PermissionArn ram:PermissionResourceType	
ListPermissionVersions	Concede permissão para listar as versões de uma permissão de AWS RAM	Lista			
ListPermissions	Concede permissão para listar as permissões AWS de RAM	Lista			
ListPrincipals	Concede permissão para listar os principais com os quais você compartilhou recursos ou que compartilharam recursos com você	Lista			
ListReplacePermissionAssociationsWork	Concede permissão para recuperar o status da substituição de permissão assíncrona	Lista			
ListResourceSharePermissions	Concede permissão para listar as Permissões associadas a um compartilhamento de recursos	Lista	resource-share*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals	
ListResourceTypes	Concede permissão para listar os tipos de recursos compartilháveis suportados pela RAM AWS	Lista			
ListResources	Concede permissão para listar os recursos que você adicionou aos compartilhamentos de recursos ou aos recursos compartilhados com você	Lista			
PromotePermissionCreatedFromPolicy	Concede permissão para criar uma permissão gerenciada pelo cliente separada e totalmente gerenciável	Gravar	customer-managed-permission*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ram:PermissionArn ram:PermissionResourceType	
PromoteResourceShareCreatedFromPolicy	Concede permissão para promover o compartilhamento de recursos especificado	Write	resource-share*		
RejectResourceShareInvitation	Concede permissão para rejeitar o convite de compartilhamento de recursos especificado	Gravar	resource-share-invitation*		
				ram:ShareOwnerAccountId ram:ResourceShareName	
ReplacePermissionAssociations	Concede permissão para atualizar todos os compartilhamentos de recursos para uma nova permissão	Gravar	customer-managed-permission*		
			permission*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ram:PermissionArn ram:PermissionResourceType	
SetDefaultPermissionVersion	Concede permissão para especificar um número de versão como a versão padrão para a respectiva permissão gerenciada pelo cliente	Gravar	customer-managed-permission*		
				ram:PermissionArn ram:PermissionResourceType	
TagResource	Concede permissão para marcar o compartilhamento de recursos ou a permissão especificada	Tags	customer-managed-permission		
			resource-share		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para desmarcar o compartilhamento de recursos ou a permissão especificada	Tags	customer-managed-permission		
			resource-share		
				aws:TagKeys	
UpdateResourceShare	Concede permissão para atualizar atributos do compartilhamento de recursos	Gravar	resource-share*		
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals ram:RequestedAllowsExternalPrincipals	

Tipos de recursos definidos pelo AWS Resource Access Manager (RAM)

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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

Chaves de condição do AWS Resource Access Manager (RAM)

AWS O Resource Access Manager (RAM) define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas tags que são transmitidas na solicitação ao criar ou marcar um compartilhamento de recurso. Se os usuários não passarem essas etiquetas específicas ou não especificarem nenhuma etiqueta, haverá falha na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves de tag que são passadas ao criar ou marcar um compartilhamento de recurso	ArrayOfString
ram:AllowsExternalPrincipals	Filtra o acesso por compartilhamentos de recursos que permitem ou negam o compartilhamento com entidades principais externas. Por exemplo, especifique true se a ação só puder ser executada em compartilhamentos de recursos que permitem o compartilhamento com entidades principais externas. Diretores externos são AWS contas que estão fora de sua organização AWS	Bool
ram:PermissionArn	Filtra o acesso pelo ARN de permissão especificado	ARN

Chaves de condição	Descrição	Tipo
ram:PermissionResourceType	Filtra o acesso por permissões do tipo de recurso especificado	String
ram:Principal	Filtra o acesso por formato do principal especificado	String
ram:RequestedAllowsExternalPrincipals	Filtra o acesso pelo valor especificado para 'allowExternalPrincipals'. Diretores externos são AWS contas que estão fora de sua organização AWS	Bool
ram:RequestedResourceType	Filtra o acesso pelo tipo de recurso especificado	String
ram:ResourceArn	Filtra o acesso pelo ARN especificado	ARN
ram:ResourceShareName	Filtra o acesso por um compartilhamento de recurso com o nome especificado	String
ram:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	String
ram:ShareOwnerAccountId	Filtra o acesso por compartilhamentos de recursos pertencentes a uma conta específica. Por exemplo, você pode usar essa chave de condição para especificar quais convites de compartilhamento de recursos podem ser aceitos ou rejeitados com base no ID da conta do proprietário do compartilhamento do recurso	String

Ações, recursos e chaves de condição do AWS Resource Explorer

AWS O Resource Explorer (prefixo do serviço:`resource-explorer-2`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Resource Explorer
- Tipos de recursos definidos pelo AWS Resource Explorer
- Chaves de condição do AWS Resource Explorer

Ações definidas pelo AWS Resource Explorer

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar

a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateDefaultView	Concede permissão para definir a visualização especificada como padrão para isso Região da AWS neste Conta da AWS	Gravar			
BatchGetView	Concede permissão para recuperar detalhes sobre visualizações que você especifica por meio de uma lista de ARNs	Leitura			resource-explorer-2:GetView

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateIndex	Concede permissão para ativar o Resource Explorer Região da AWS na qual você chamou essa operação criando um índice.	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateManagedView [somente permissão]	Concede permissão para criar uma visualização gerenciada	Gravar			
CreateView	Concede permissão para criar uma exibição que os usuários possam consultar	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteIndex	Concede permissão para desativar o Resource Explorer no especificado Região da AWS excluindo o índice	Gravar	index*		
DeleteResourcePolicy [somente permissão]	Concede permissão para excluir a política de recurso da exibição especificada	Gerenciamento de permissões	view*		
DeleteView	Concede permissão para excluir uma exibição	Gravar	view*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateDefaultView	Concede permissão para remover a visualização padrão da Região da AWS na qual você chama essa operação	Gravar			
GetAccountLevelServiceConfiguration	Concede permissão ao Resource Explorer para acessar dados em nível de conta em sua AWS organização	Leitura			
GetDefaultView	Concede permissão para recuperar o nome do recurso Amazon (ARN) da visualização que é o padrão para Região da AWS a qual você chama essa operação	Leitura			
GetIndex	Concede permissão para recuperar informações sobre o índice Região da AWS no qual você chama essa operação	Leitura			
GetManagedView	Concede permissão para obter a visualização gerenciada	Leitura	managed-view*		
GetResourcePolicy [somente permissão]	Concede permissão para recuperar informações sobre a política de recursos da exibição especificada	Leitura	view*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetView	Concede permissão para recuperar informações sobre a exibição especificada	Leitura	view*		
ListIndexes	Concede permissão para listar os índices em todos Regiões da AWS	Lista			
ListIndexesForMembers	Concede permissão para listar os índices da conta do membro da organização em todos Regiões da AWS	Lista			
ListManagedViews	Concede permissão para listar visualizações gerenciadas	Lista			
ListSupportedResourceTypes	Concede permissão para recuperar uma lista de todos tipos de recursos com suporte no Resource Explorer no momento	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas anexadas ao recurso especificado	Leitura	index view		
ListViews	Concede permissão para listar os nomes de recursos da Amazon (ARNs) de todas as visualizações disponíveis Região da AWS nas quais você chama essa operação	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutResourcePolicy [somente permissão]	Concede permissão para atualizar a política de recursos da exibição especificada	Gerenciamento de permissões	view*		
Search	Concede permissão para pesquisar recursos e exibir detalhes sobre todos os recursos que correspondem aos critérios especificados	Leitura	view*		
				resource-explorer-2:Operation	
TagResource	Concede permissão para adicionar um ou mais pares de chave e valor de etiquetas ao recurso especificado	Tags	index		
			view		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover um ou mais pares de chave e valor de etiquetas do recurso especificado	Tags	index		
			view		
				aws:TagKeys	
UpdateIndexType	Concede permissão para alterar o tipo do índice de LOCAL para AGGREGATOR ou vice-versa	Gravar	index*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateView	Concede permissão para modificar alguns dos detalhes de uma exibição	Gravar	view*		

Tipos de recursos definidos pelo AWS Resource Explorer

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}`	

Chaves de condição do AWS Resource Explorer

AWS O Resource Explorer define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas chaves de etiquetas anexadas ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString
resource-explorer-2:Operation	Filtra o acesso pela operação real que está sendo invocada, valores disponíveis: Pesquisar, ListResources	String

Ações, recursos e chaves de condição da API de marcação de resource groups da Amazon

A API de marcação por etiquetas de resource groups da Amazon (prefixo do serviço: `tag`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.

- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela API de marcação por etiquetas de resource groups da Amazon
- Tipos de recursos definidos pela API de marcação de resource groups da Amazon
- Chaves de condição da API de marcação de resource groups da Amazon

Ações definidas pela API de marcação por etiquetas de resource groups da Amazon

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeReportCreation	Concede permissão para descrever o status da StartReportCreation operação	Leitura			
GetComplianceSummary	Concede permissão para recuperar um resumo de quantos recursos não estão em conformidade com as políticas da etiqueta em vigor	Leitura			
GetResources	Concede permissão para retornar recursos marcados ou marcados anteriormente na conta especificada Região da AWS para a conta de chamada	Leitura			
GetTagKeys	Concede permissão para devolver as chaves de tag atualmente em uso na conta	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	especificada Região da AWS para a chamada				
GetTagValues	Concede permissão para retornar valores de tag para a chave especificada que são usados na conta especificada Região da AWS para a chamada	Leitura			
StartReportCreation	Concede permissão para iniciar a geração de um relatório listando todos os recursos marcados em contas em toda a organização e indicando se cada recurso está em conformidade com a política de etiquetas em vigor	Gravar			
TagResources	Concede permissão para aplicar uma ou mais etiquetas ao recurso especificado	Tags			
UntagResources	Concede permissão para remover as etiquetas especificadas dos recursos especificados	Tags			

Tipos de recursos definidos pela API de marcação de resource groups da Amazon

A API de marcação por etiquetas de resource groups da Amazon não oferece suporte à especificação do ARN de um recurso no elemento `Resource` de uma instrução de política do IAM.

Para conceder acesso à API de marcação por etiquetas de resource groups da Amazon, especifique `"Resource": "*"` na política.

Chaves de condição da API de marcação de resource groups da Amazon

A Marcação por etiquetas de resource groups não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Resource Groups

AWS Os Resource Groups (prefixo do serviço:`resource-groups`) fornecem os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Resource Groups
- Tipos de recursos definidos pelo AWS Resource Groups
- Chaves de condição do AWS Resource Groups

Ações definidas pelo AWS Resource Groups

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o

nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
Associate Resource	Concede permissão para associar um recurso a uma Aplicação	Gravar	group*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
[somente permissão]					
CancelTagSyncTask	Concede permissão para cancelar uma tarefa de sincronização de tags de um grupo de aplicações	Gravar	group*		resource-groups:DeleteGroup
CreateGroup	Concede permissão para criar um grupo de recursos com um nome, descrição e consulta de recurso especificados	Write		aws:RequestTag/${TagKey} aws:TagKeys	cloudformation:DescribeStacks
DeleteGroup	Concede permissão para excluir um grupo de recursos especificado	Gravar	group*		tag:GetResources
DeleteGroupPolicy [somente permissão]	Concede permissão para excluir uma política baseada em recursos do grupo especificado	Gravar	group*		
DisassociateResource [somente permissão]	Concede permissão para desassociar um recurso de uma Aplicação	Gravar	group*		
GetAccountSettings	Concede permissão para obter o status atual de recursos opcionais em Resource Groups	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetGroup	Concede permissão para obter informações de um grupo de recursos especificado	Read	group*		
GetGroupConfiguration	Concede permissão para obter a configuração do serviço associada ao grupo de recursos especificado	Leitura	group*		
GetGroupPolicy [somente permissão]	Concede permissão para obter uma política baseada em recursos para o grupo especificado	Leitura	group*		
GetGroupQuery	Concede permissão para obter a consulta associada a um grupo de recursos especificado	Leitura	group*		
GetTagSyncTask	Concede permissão para obter informações de uma tarefa de sincronização de tags especificada	Leitura	group*		
GetTags	Concede permissão para obter as etiquetas associadas a um grupo de recursos especificado	Read	group*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GroupResources	Concede permissão para adicionar os recursos especificados ao grupo especificado	Write	group*		resource-groups:Tag tag:TagResources
ListGroupResources	Concede permissão para listar os recursos que são membros de um grupo de recursos especificado	Lista	group*		cloudformation:DescribeStacks cloudformation:ListStackResources tag:GetResources
ListGroupingStatuses	Concede permissão para listar os status de agrupamento de um grupo de aplicações especificado	Lista	group*		
ListGroups	Concede permissão para listar todos os grupos de recursos em sua conta	Lista			
ListResourceTypes [somente permissão]	Concede permissão para listar tipos de recursos compatíveis	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagSyncTasks	Concede permissão para listar todas as tarefas de sincronização de tags na sua conta	Lista	group*		
PutGroupConfiguration	Concede permissão para colocar a configuração de serviço associada ao grupo de recursos especificado	Write	group*		
PutGroupPolicy [somente permissão]	Concede permissão para adicionar uma política baseada em recursos para o grupo especificado	Gravar	group*		
SearchResources	Concede permissão para pesquisar AWS recursos que correspondam à consulta fornecida	Lista			cloudformation:DescribeStacks cloudformation:ListStackResources tag:GetResources
StartTagSyncTask	Concede permissão para criar uma tarefa de sincronização de tags de um grupo de aplicações	Gravar	group*		iam:PassRole resource-groups:CreateGroup

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
Tag	Concede permissão para marcar um grupo de recursos especificado	Marcação	group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UngroupResources	Concede permissão para remover os recursos especificados do grupo especificado	Write	group*		resource-groups:Untag tag:UntagResources
Untag	Concede permissão para remover etiquetas associadas a um grupo de recursos especificado	Tags	group*		
				aws:TagKeys	
UpdateAccountSettings	Concede permissão para atualizar recursos opcionais em Resource Groups	Gravar			
UpdateGroup	Concede permissão para atualizar um grupo de recursos especificado	Write	group*		
UpdateGroupQuery	Concede permissão para atualizar a consulta associada a um grupo de recursos especificado	Write	group*		cloudformation:DescribeStacks

Tipos de recursos definidos pelo AWS Resource Groups

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS Resource Groups

AWS Resource Groups define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon RHEL Knowledgebase Portal

O Amazon RHEL Knowledgebase Portal (prefixo do serviço: `rhelkb`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon RHEL Knowledgebase Portal
- Tipos de recursos definidos pelo Amazon RHEL Knowledgebase Portal
- Chaves de condição para o Amazon RHEL Knowledgebase Portal

Ações definidas pelo Amazon RHEL Knowledgebase Portal

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetRhelURL	Concede permissão para acessar o Amazon RHEL Knowledgebase Portal	Leitura			

Tipos de recursos definidos pelo Amazon RHEL Knowledgebase Portal

O Amazon RHEL Knowledgebase Portal não oferece suporte à especificação do ARN de um recurso no elemento `Resource` de uma instrução de política do IAM. Para conceder acesso ao Amazon RHEL Knowledgebase Portal, especifique `"Resource": "*"` em sua política.

Chaves de condição para o Amazon RHEL Knowledgebase Portal

O RHEL KB não tem chaves de contexto específicas do serviço que possam ser usadas no elemento `Condition` de instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o AWS RoboMaker

AWS RoboMaker (prefixo do serviço:`robomaker`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS RoboMaker
- Tipos de recursos definidos pelo AWS RoboMaker
- Chaves de condição do AWS RoboMaker

Ações definidas pelo AWS RoboMaker

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchDeleteWorlds	Excluir um ou mais mundos em uma operação em lote	Write			
BatchDescribeSimulationJob	Descrever vários trabalhos de simulação	Read			
CancelDeploymentJob	Cancelar um trabalho de implantação	Write	deploymentJob*		
CancelSimulationJob	Cancelar um trabalho de simulação	Write	simulationJob*		
CancelSimulationJobBatch	Cancelar um lote de trabalhos de simulação	Write	simulationJobBatch*		
CancelWorldExportJob	Cancelar um trabalho de exportação de mundos	Write	worldExportJob*		
CancelWorldGenerationJob	Cancelar um trabalho de geração de mundos	Write	worldGenerationJob*		
CreateDeploymentJob	Criar um trabalho de implantação	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateFleet	Criar uma frota de implantação que representa um grupo lógico de robôs que executam o mesmo aplicativo de robô	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateRobot	Criar um robô que pode ser registrado em uma frota	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
CreateRobotApplication	Criar um aplicativo de robô	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateRobotApplicationVersion	Criar um snapshot de um aplicativo de robô	Write	robotApplication*		s3:GetObject
CreateSimulationApplication	Criar um aplicativo de simulação	Write		aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSimulationApplicationVersion	Criar um snapshot de um aplicativo de simulação	Write	simulationApplication*		s3:GetObject
CreateSimulationJob	Criar uma trabalho de simulação	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
CreateWorldExportJob	Criar um trabalho de exportação de mundos	Write	world*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateWorldGenerationJob	Criar um trabalho de geração de mundos	Write	worldTemplate*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateWorldTemplate	Criar um modelo de mundo	Write		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteFleet	Excluir uma frota de implantação	Write	deploymentFleet*		
DeleteRobot	Excluir um robô	Write	robot*		
DeleteRobotApplication	Excluir um aplicativo de robô	Write	robotApplication*		
DeleteSimulationApplication	Excluir um aplicativo de simulação	Write	simulationApplication*		
DeleteWorldTemplate	Excluir um modelo de mundo	Write	worldTemplate*		
DeregisterRobot	Cancelar o registro de um robô em uma frota	Write	deploymentFleet* robot*		
DescribeDeploymentJob	Descrever um trabalho de implantação	Read	deploymentJob*		
DescribeFleet	Descrever uma frota de implantação	Read	deploymentFleet*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeRobot	Descrever um robô	Read	robot*		
DescribeRobotApplication	Descrever um aplicativo de robô	Read	robotApplication*		
DescribeSimulationApplication	Descrever um aplicativo de simulação	Read	simulationApplication*		
DescribeSimulationJob	Descrever um trabalho de simulação	Read	simulationJob*		
DescribeSimulationJobBatch	Descrever um lote de trabalhos de simulação	Read	simulationJobBatch*		
DescribeWorld	Descrever um mundo	Read	world*		
DescribeWorldExportJob	Descrever um trabalho de exportação de mundos	Read	worldExportJob*		
DescribeWorldGenerationJob	Descrever um trabalho de geração de mundos	Read	worldGenerationJob*		
DescribeWorldTemplate	Descrever um modelo de mundo	Read	worldTemplate*		
GetWorldTemplateBody	Obter o corpo de um modelo de mundo	Read	worldTemplate*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDeploymentJobs	Listar trabalhos de implantação	List			
ListFleets	Listar frotas	List			
ListRobotApplications	Listar aplicativos de robô	List			
ListRobots	Listar robôs	List			
ListSimulationApplications	Listar aplicativos de simulação	List			
ListSimulationJobBatches	Listar lotes de trabalhos de simulação	List			
ListSimulationJobs	Listar trabalhos de simulação	List			
ListSupportedAvailabilityZones [somente permissão]	Lista as zonas de disponibilidade compatíveis	Lista			
ListTagsForResource	Listar tags para um RoboMaker recurso	Lista	deploymentFleet		
			deploymentJob		
			robot		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			robotApplication		
			simulationApplication		
			simulationJob		
			simulationJobBatch		
			world		
			worldExportJob		
			worldGenerationJob		
			worldTemplate		
ListWorldExportJobs	Listar trabalhos de exportação de mundos	List			
ListWorldGenerationJobs	Listar trabalhos de geração de mundos	List			
ListWorldTemplates	Listar modelos de mundos	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListWorlds	Listar mundos	List			
RegisterRobot	Registrar um robô em uma frota	Write	deploymentFleet*		
			robot*		
RestartSimulationJob	Reiniciar um trabalho de simulação em execução	Write	simulationJob*		
StartSimulationJobBatch	Criar um lote de trabalhos de simulação	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
SyncDeploymentJob	Garante que o aplicativo de robô implantado mais recentemente seja implantado em todos os robôs da frota	Gravar	deploymentFleet*		iam:CreateServiceLinkedRole
TagResource	Adicionar tags a um RoboMaker recurso	Tags	deploymentFleet		
			deploymentJob		
			robot		
			robotApplication		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			simulationApplication		
			simulationJob		
			simulationJobBatch		
			world		
			worldExportJob		
			worldGenerationJob		
			worldTemplate		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Remover tags de um RoboMaker recurso	Tags	deploymentFleet		
			deploymentJob		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			robot		
			robotApplication		
			simulationApplication		
			simulationJob		
			simulationJobBatch		
			world		
			worldExportJob		
			worldGenerationJob		
			worldTemplate		
				aws:TagKeys	
UpdateRobotApplication	Atualizar um aplicativo de robô	Write	robotApplication*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateRobotDeployment [somente permissão]	Relatar o status de implantação de um robô individual	Write			
UpdateSimulationApplication	Atualizar um aplicativo de simulação	Write	simulationApplication*		
UpdateWorldTemplate	Atualizar um modelo de mundo	Gravar	worldTemplate*		

Tipos de recursos definidos pelo AWS RoboMaker

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Tipos de recursos	ARN	Chaves de condição
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/${TagKey}
worldTemplate	arn:${Partition}:robomaker:${Region}:${Account}:world-template/${WorldTemplateJobId}	aws:ResourceTag/${TagKey}
world	arn:${Partition}:robomaker:${Region}:${Account}:world/${WorldId}	aws:ResourceTag/${TagKey}

Chaves de condição do AWS RoboMaker

AWS RoboMaker define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base nas etiquetas transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra as ações com base nas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra ações com base nas chaves da etiqueta transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Route 53

O Amazon Route 53 (prefixo do serviço: `route53`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Route 53

- Tipos de recursos definidos pelo Amazon Route 53
- Chaves de condição do Amazon Route 53

Ações definidas pelo Amazon Route 53

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ActivateKeySigningKey	Concede permissão para ativar uma chave de assinatura de chaves para que ela possa ser usada para assinatura pelo DNSSEC	Write	hostedzone*		
AssociateVPCWithHostedZone	Concede permissão para associar uma Amazon VPC adicional a uma zona hospedada privada	Gravar	hostedzone		ec2:DescribeVpcs
				route53:VPCs	
ChangeCidrCollection	Concede permissão para criar ou excluir blocos CIDR em uma coleção de CIDR	Gravar	cidrcollection*		
ChangeResourceRecordSets	Concede permissão para criar, atualizar ou excluir um registro que contém informações do DNS autoritativo para um nome de domínio ou de subdomínio especificado	Write	hostedzone*		
				route53:ChangeResourceRecordSetsNormalizedRecordNames route53:ChangeResc	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				urceRecordSetsRecordTypes route53:ChangeResourceRecordSetsActions	
ChangeTagsForResource	Concede permissão para adicionar, editar ou excluir etiquetas de uma verificação de integridade ou de uma zona hospedada	Tags	healthcheck*		
			hostedzone*		
CreateCidrCollection	Concede permissão para criar uma nova coleção de CIDR	Gravar			
CreateHealthCheck	Concede permissão para criar uma nova verificação de integridade que monitora a integridade e a performance das suas aplicações Web, servidores Web e outros recursos	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateHostedZone	Concede permissão para criar uma zona hospedada pública que você usa para especificar como o Domain Name System (DNS) roteia o tráfego na Internet para um domínio, como example.com, e seus subdomínios	Write		route53:VPCs	ec2:DescribeVpcs
CreateKeySigningKey	Concede permissão para criar uma nova chave de assinatura de chaves associada a uma zona hospedada	Write	hostedzone*		
CreateQueryLoggingConfig	Concede permissão para criar uma configuração para o log de consultas DNS	Write	hostedzone*		
CreateReusableDelegationSet	Concede permissão para criar um conjunto de delegações (um grupo de quatro servidores de nome) que podem ser reutilizadas por várias zonas hospedadas	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateTrafficPolicy	Concede permissão para criar uma política de tráfego que você usa para criar vários registros DNS para um nome de domínio (como example.com) ou um nome de subdomínio (como www.example.com)	Write			
CreateTrafficPolicyInstance	Concede permissão para criar registros em uma zona hospedada especificada com base nas configurações em uma versão de política de tráfego especificada	Write	hostedzone* trafficpolicy*		
CreateTrafficPolicyVersion	Concede permissão para criar uma nova versão de uma política de tráfego existente	Gravar	trafficpolicy*		
CreateVPCAssociationAuthorization	Concede permissão para autorizar a pessoa Conta da AWS que criou uma VPC específica a enviar uma solicitação de associado, que VPCWith HostedZone associa a VPC a uma zona hospedada especificada que foi criada por uma conta diferente	Gravar	hostedzone* 	 route53:VPCs	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeactivateKeySigningKey	Concede permissão para desativar uma chave de assinatura de chave para que ela não seja usada para assinatura pelo DNSSEC	Gravar	hostedzone*		
DeleteCidrCollection	Concede permissão para excluir uma coleção de CIDR	Gravar	cidrcollection*		
DeleteHealthCheck	Concede permissão para excluir uma verificação de integridade	Write	healthcheck*		
DeleteHostedZone	Concede permissão para excluir uma zona hospedada	Write	hostedzone*		
DeleteKeySigningKey	Concede permissão para excluir uma chave de assinatura de chaves	Write	hostedzone*		
DeleteQueryLoggingConfig	Concede permissão para excluir uma configuração do log de consultas DNS	Write	queryloggingconfig*		
DeleteReusableDelegationSet	Concede permissão para excluir um conjunto de delegações reutilizáveis	Write	delegationset*		
DeleteTrafficPolicy	Concede permissão para excluir uma política de tráfego	Write	trafficpolicy*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteTrafficPolicyInstance	Concede permissão para excluir uma instância de política de tráfego e todos os registros que o Route 53 criou quando você criou a instância	Write	trafficpolicyinstance*		
DeleteVPCAssociationAuthorization	Concede permissão para remover a autorização para a associação de uma Amazon Virtual Private Cloud com uma zona hospedada privada do Route 53	Write	hostedzone*		
				route53:VPCs	
DisableHostedZoneDNSSEC	Concede permissão para desativar a assinatura DNSSEC em uma zona hospedada específica	Write	hostedzone*		
DisassociateVPCFromHostedZone	Concede permissão para desassociar Amazon Virtual Private Cloud de uma zona hospedada privada do Route 53	Write	hostedzone		ec2:DescribeVpcs
				route53:VPCs	
EnableHostedZoneDNSSEC	Concede permissão para habilitar a assinatura DNSSEC em uma zona hospedada específica	Write	hostedzone*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAccountLimit	Concede permissão para obter o limite especificado para a conta atual, por exemplo, o número máximo de verificações de integridade que você pode criar usando a conta	Read			
GetChange	Concede permissão para obter o status atual de uma solicitação para criar, atualizar ou excluir um ou mais registros	List	change*		
GetCheckerIpRanges	Concede permissão para obter uma lista dos intervalos IP usados pelos verificadores de integridade do Route 53 para verificar a integridade de seus recursos	List			
GetDNSSEC	Concede permissão para obter informações sobre o DNSSEC para uma zona hospedada específica, incluindo as chaves de assinatura de chaves na zona hospedada	Read	hostedzone*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetGeoLocation	Concede permissão para obter informações sobre se uma geolocalização especificada é suportada para registros de geolocalização do Route 53	List			
GetHealthCheck	Concede permissão para obter informações sobre uma verificação de integridade especificada	Leitura	healthcheck*		
GetHealthCheckCount	Concede permissão para obter o número de verificações de saúde associadas à atual Conta da AWS	Lista			
GetHealthCheckLastFailureReason	Concede permissão para obter o motivo da falha mais recente de uma verificação de integridade especificada	List	healthcheck*		
GetHealthCheckStatus	Concede permissão para obter o status de uma verificação de integridade especificada	List	healthcheck*		
GetHostedZone	Concede permissão para obter informações sobre uma zona hospedada especificada incluindo os quatro servidores de nome que o Route 53 atribuiu à zona hospedada	Lista	hostedzone*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetHostedZoneCount	Concede permissão para obter o número de zonas hospedadas associadas à atual Conta da AWS	Lista			
GetHostedZoneLimit	Concede permissão para obter o limite especificado de uma zona hospedada especificada	Read	hostedzone*		
GetQueryLoggingConfig	Concede permissão para obter informações sobre a configuração especificada do log de consultas DNS	Read	queryloggingconfig*		
GetReusableDelegationSet	Concede permissão para obter informações sobre um conjunto de delegações reutilizáveis especificado incluindo os quatro servidores atribuídos ao conjunto de delegações	List	delegationset*		
GetReusableDelegationSetLimit	Concede permissão para obter o número máximo de zonas hospedadas que você pode associar ao conjunto de delegações reutilizáveis especificado	Read	delegationset*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetTrafficPolicy	Concede permissão para obter informações sobre uma versão de política de tráfego especificada	Read	trafficpolicy*		
GetTrafficPolicyInstance	Concede permissão para obter informações sobre uma instância de política de tráfego especificada	Leitura	trafficpolicyinstance*		
GetTrafficPolicyInstanceCount	Concede permissão para obter o número de instâncias da política de tráfego associadas à atual Conta da AWS	Leitura			
ListCidrBlocks	Concede permissão para obter uma lista dos blocos CIDR em uma coleção de CIDR especificada	Lista	cidrcollection*		
ListCidrCollections	Concede permissão para obter uma lista das coleções CIDR associadas à atual Conta da AWS	Lista			
ListCidrLocations	Concede permissão para obter uma lista dos locais de CIDR que pertencem a uma coleção de CIDR especificada	Lista	cidrcollection*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListGeoLocations	Concede permissão para obter uma lista de localizações geográficas para as quais o Route 53 oferece suporte para geolocalização	Leitura			
ListHealthChecks	Concede permissão para obter uma lista das verificações de saúde associadas à atual Conta da AWS	Leitura			
ListHostedZones	Concede permissão para obter uma lista das zonas hospedadas públicas e privadas associadas à atual Conta da AWS	Lista			
ListHostedZonesByName	Concede permissão para obter uma lista de suas zonas hospedadas em ordem lexicográfica. As zonas hospedadas são classificadas por nome com os rótulos invertidos, por exemplo, com.example.www	Lista			
ListHostedZonesByVPC	Concede permissão para obter uma lista de todas as zonas hospedadas privadas às quais uma VPC especificada está associada	Lista		route53:VPCs	ec2:DescribeVpcs

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListQueryLoggingConfigs	Concede permissão para listar as configurações do registro de consultas DNS associadas à atual Conta da AWS ou à configuração associada a uma zona hospedada especificada	Lista	hostedzone		
ListResourceRecordSets	Concede permissão para listar os registros em uma zona hospedada especificada	Lista	hostedzone*		
ListReusableDelegationSets	Concede permissão para listar os conjuntos de delegações reutilizáveis associados à Conta da AWS atual.	Leitura			
ListTagsForResource	Concede permissão para listar as etiquetas de uma verificação de integridade ou zona hospedada	Leitura	healthcheck		
			hostedzone		
ListTagsForResources	Concede permissão para listar etiquetas de até 10 verificações de integridade ou de zonas hospedadas	Leitura	healthcheck		
			hostedzone		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTrafficPolicies	Concede permissão para obter informações sobre a versão mais recente de cada política de tráfego associada à Conta da AWS atual. As políticas são listadas na ordem em que foram criadas	Lista			
ListTrafficPolicyInstances	Concede permissão para obter informações sobre as instâncias da política de tráfego que você criou usando o atual Conta da AWS	Leitura			
ListTrafficPolicyInstancesByHostedZone	Concede permissão para obter informações sobre as instâncias de política de tráfego que você criou em uma zona hospedada especificada	List	hostedzone*		
ListTrafficPolicyInstancesByPolicy	Concede permissão para obter informações sobre as instâncias de política de tráfego que você criou usando uma versão da política de tráfego especificada	List	trafficpolicy*		
ListTrafficPolicyVersions	Concede permissão para obter informações sobre todas as versões de uma política de tráfego especificada	Lista	trafficpolicy*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListVPCAssociationAuthorizations	Concede permissão para obter uma lista das VPCs que foram criadas por outras contas e que podem ser associadas a uma zona hospedada especificada	Lista	hostedzone*		
TestDNSAnswer	Concede permissão para obter o valor que o Route 53 retorna em resposta a uma consulta DNS de um nome e tipo de registro especificados	Read			
UpdateHealthCheck	Concede permissão para atualizar uma verificação de integridade existente	Write	healthcheck*		
UpdateHostedZoneComment	Concede permissão para atualizar os comentários de uma zona hospedada especificada	Write	hostedzone*		
UpdateTrafficPolicyComment	Concede permissão para atualizar os comentários de uma versão de política de tráfego especificada	Write	trafficpolicy*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateTrafficPolicyInstance	Concede permissão para atualizar registros em uma zona hospedada especificada que foi criada com base nas configurações em uma versão de política de tráfego especificada	Write	trafficpolicyinstance*		

Tipos de recursos definidos pelo Amazon Route 53

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
cidrcollection	`arn:${Partition}:route53:::cidrcollection/${Id}`	
change	`arn:${Partition}:route53:::change/${Id}`	
delegationset	`arn:${Partition}:route53:::delegationset/${Id}`	
healthcheck	`arn:${Partition}:route53:::healthcheck/${Id}`	

Tipos de recursos	ARN	Chaves de condição
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}	

Chaves de condição do Amazon Route 53

O Amazon Route 53 define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
route53:ChangeResourceRecordSetsActions	Filtra o acesso pelas ações de alteração, CREATE, UPSERT ou DELETE, em uma solicitação ChangeResourceRecordSets	ArrayOfString
route53:ChangeReso	Filtra o acesso pelos nomes de registros DNS normalizados em uma solicitação ChangeResourceRecordSets	ArrayOfString

Chaves de condição	Descrição	Tipo
urceRecordSetsNormalizedRecordNames		
route53:ChangeResourceRecordSetsRecordTypes	Filtra o acesso pelos tipos de registro DNS em uma solicitação ChangeResourceRecordSets	ArrayOfString
route53:VPCs	Filtra o acesso por VPCs solicitação	String

Ações, recursos e chaves de condição para domínios do Amazon Route 53

Os domínios do Amazon Route 53 (prefixo de serviço: `route53domains`) fornecem os recursos específicos de serviço, ações e chaves de contexto de condição a seguir para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas por domínios do Amazon Route 53
- Tipos de recursos definidos por domínios do Amazon Route 53
- Chaves de condição para domínios do Amazon Route 53

Ações definidas por domínios do Amazon Route 53

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptDomainTransferFromAnotherAwsAccount	Concede permissão para aceitar a transferência de um domínio de outro Conta da AWS para o atual Conta da AWS	Gravar			
AssociateDelegationSignerToDomain	Concede permissão para associar um novo signatário da delegação a um domínio	Gravar			
CancelDomainTransferToAnotherAwsAccount	Concede permissão para cancelar a transferência de um domínio do atual Conta da AWS para outro Conta da AWS	Gravar			
CheckDomainAvailability	Concede permissão para verificar a disponibilidade de um nome de domínio	Read			
CheckDomainTransferability	Concede permissão para verificar se um nome de domínio pode ser transferido para o Amazon Route 53	Leitura			
DeleteDomain	Concede permissão para excluir domínios	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteTagsForDomain	Concede permissão para excluir as etiquetas especificadas de um domínio	Marcação			
DisableDomainAutoRenew	Concede permissão para configurar o Amazon Route 53 para renovar automaticamente o domínio especificado antes que o registro do domínio expire	Gravar			
DisableDomainTransferLock	Concede permissão para remover o bloqueio de transferência no domínio (especificamente o clientTransferProhibited status) para permitir transferências de domínio	Gravar			
DisassociateDelegationSignerFromDomain	Concede permissão para desassociar um signatário existente da delegação de um domínio	Gravar			
EnableDomainAutoRenew	Concede permissão para configurar o Amazon Route 53 para renovar automaticamente o domínio especificado antes que o registro do domínio expire	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
EnableDomainTransferLock	Concede permissão para definir o bloqueio de transferência no domínio (especificamente o clientTransferProhibited status) para evitar transferências de domínio	Gravar			
GetContactReachabilityStatus	Concede permissão para obter informações sobre se o contato do registrante respondeu em operações que necessitam de confirmação de que o endereço de e-mail do contato do registrante é válido, como o registro de um novo domínio	Leitura			
GetDomainDetail	Concede permissão para obter informações detalhadas sobre um domínio	Read			
GetDomainSuggestions	Concede permissão para obter uma lista de nomes de domínio sugeridos considerando uma string, que pode ser um nome de domínio ou simplesmente uma palavra ou frase (sem espaços)	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetOperationDetail	Concede permissão para obter o status atual de uma operação que não está concluída	Leitura			
ListDomains	Concede permissão para listar todos os nomes de domínio registrados no Amazon Route 53 atualmente Conta da AWS	Lista			
ListOperations	Concede permissão para listar a operação IDs de operações que ainda não foram concluídas	Lista			
ListPrices	Concede permissão para listar os preços das operações para TLDs	Lista			
ListTagsForDomain	Concede permissão para listar todas as etiquetas associadas ao domínio especificado	Leitura			
PushDomain	Concede permissão para alterar a etiqueta IPS do domínio .uk para iniciar um processo de transferência do Route 53 para outro registrador	Gravar			
RegisterDomain	Concede permissão para registrar domínios	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RejectDomainTransferFromAnotherAwsAccount	Concede permissão para rejeitar a transferência de um domínio de outro Conta da AWS para o atual Conta da AWS	Gravar			
RenewDomain	Concede permissão para renovar domínios para o número especificado de anos	Gravar			
ResendContactReachabilityEmail	Concede permissão para reenviar o e-mail de confirmação ao endereço de e-mail atual do contato do registrante em operações que necessitam de confirmação de que o endereço de e-mail do contato do registrante é válido, como registrar um novo domínio	Gravar			
ResendOperationAuthorization	Concede permissão para reenviar a autorização de operação	Gravar			
RetrieveDomainAuthCode	Concede permissão para obter o AuthCode para o domínio	Gravar			
TransferDomain	Concede permissão para transferir um domínio de outro registrador para o Amazon Route 53	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TransferDomainToAnotherAwsAccount	Concede permissão para transferir um domínio do atual Conta da AWS para outro Conta da AWS	Gravar			
UpdateDomainContact	Concede permissão para atualizar as informações de contato do domínio	Write			
UpdateDomainContactPrivacy	Concede permissão para atualizar a configuração de privacidade de contato do domínio	Write			
UpdateDomainNameservers	Concede permissão para substituir o conjunto atual de servidores de nome de um domínio pelo conjunto de servidores de nome especificado	Write			
UpdateTagsForDomain	Concede permissão para adicionar ou atualizar etiquetas de um domínio especificado	Tags			
ViewBilling	Concede permissão para obter todos os registros de cobrança relacionados ao domínio atuais Conta da AWS por um período especificado	Leitura			

Tipos de recursos definidos por domínios do Amazon Route 53

Os domínios do Amazon Route 53 não oferecem suporte à especificação do ARN de um recurso no elemento `Resource` de uma declaração de política do IAM. Para permitir o acesso a domínios do Amazon Route 53, especifique `"Resource": "*"` em sua política.

Chaves de condição para domínios do Amazon Route 53

Os domínios do Route 53 não têm chaves de contexto específicas de serviço que possam ser usadas no elemento `Condition` das instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do Amazon Route 53 Profiles

O Amazon Route 53 Profiles (prefixo do serviço: `route53profiles`) fornece os recursos, ações e chaves de contexto de condição a seguir específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Route 53 Profiles
- Tipos de recursos definidos pelo Amazon Route 53 Profiles
- Chaves de condição do Amazon Route 53 Profiles

Ações definidas pelo Amazon Route 53 Profiles

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateProfile	Concede permissão para associar um perfil à VPC do cliente	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeVpcs
AssociateResourceToProfile	Concede permissão para associar um recurso, como o grupo de regras do firewall de DNS, a zona hospedada privada, a regra de resolvedor etc., a um perfil especificado	Gravar			
CreateProfile	Concede permissão para criar um recurso de perfil	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteProfile	Concede permissão para excluir um Perfil especificado pelo ProfileId	Gravar			
DisassociateProfile	Concede permissão para excluir uma associação entre uma VPC de cliente e o perfil especificado	Gravar			
DisassociateResour	Concede permissão para excluir a associação entre o recurso, como o grupo de	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ceFromProfile	regras do firewall de DNS, a zona hospedada privada, a regra do resolvedor etc., e o perfil especificado				
GetProfile	Concede permissão para obter um perfil	Leitura			
GetProfileAssociation	Concede permissão para obter um perfil para uma associação de VPC especificada pelo ID da associação de perfil	Leitura			
GetProfilePolicy [somente permissão]	Concede permissão para ler a política de controle de acesso ao RAM de um perfil	Leitura	profile*		
GetProfileResourceAssociation	Concede permissão para obter uma associação de recursos de perfil com base no ProfileResourceAssociationId	Leitura			
ListProfileAssociations	Concede permissão para listar tudo VPCs ao qual o Perfil especificado está associado	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListProfileResourceAssociations	Concede permissão para listar todas as associações entre os recursos, como os grupos de regras do firewall de DNS, as zonas hospedadas privadas, as regras do resolvedor, etc., para o ID de perfil fornecido	Lista			
ListProfiles	Concede permissão para listar todos os perfis criados e compartilhados com o cliente	Lista			
ListTagsForResource	Concede permissão para listar todas as tags associadas ao recurso	Lista			
PutProfilePolicy [somente permissão]	Concede permissão para definir a política de controle de acesso ao RAM de um perfil	Gravar	profile*		
TagResource	Concede permissão para adicionar uma tag a um determinado recurso	Tags	profile		
			profile-association		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para excluir uma tag do recurso fornecido	Tags	profile		
			profile-association		
				aws:TagKeys	
UpdateProfileResourceAssociation	Concede permissão para atualizar o nome da associação de recursos do perfil ou as propriedades do recurso ou ambos. Se o nome e as propriedades do recurso forem nulos, a API retornará a associação de recursos do perfil existente	Gravar			

Tipos de recursos definidos pelo Amazon Route 53 Profiles

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
profile	arn:${Partition}:route53profiles:${Region}:${Account}:profile/${ResourceId}	aws:ResourceTag/${TagKey}
profile-association	arn:${Partition}:route53profiles:${Region}:${Account}:profile-association/${ResourceId}	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Route 53 Profiles

O Amazon Route 53 Profiles define as chaves de condição a seguir que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pela presença de pares chave-valor da etiqueta anexados ao recurso	Segmento
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Route 53 Recovery Cluster

O Amazon Route 53 Recovery Cluster (prefixo do serviço: `route53-recovery-cluster`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Route 53 Recovery Cluster
- Tipos de recursos definidos pelo Amazon Route 53 Recovery Cluster
- Chaves de condição para o Amazon Route 53 Recovery Cluster

Ações definidas pelo Amazon Route 53 Recovery Cluster

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar

a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetRoutingControlState	Concede permissão para obter um estado de controle de roteamento	Leitura	routingcontrol*		
ListRoutingControls	Concede permissão para listar controles de roteamento	Leitura			
UpdateRoutingControlState	Concede permissão para atualizar um estado de controle de roteamento	Gravar	routingcontrol*		
				route53-recovery-	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				cluster:AllowSafetyRulesOverrides	
UpdateRoutingControlStates	Concede permissão para atualizar um lote de estados de controle de roteamento	Gravar	routingcontrol*		
				route53-recovery-cluster:AllowSafetyRulesOverrides	

Tipos de recursos definidos pelo Amazon Route 53 Recovery Cluster

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
routingcontrol	`arn:${Partition}:route53-recovery-control::${Account}:controlpanel/${ControlPanelId}/routingcontrol/${RoutingControlId}`	

Chaves de condição para o Amazon Route 53 Recovery Cluster

O Amazon Route 53 Recovery Cluster define as chaves de condição a seguir que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
route53-recovery-cluster:AllowSafetyRulesOverrides	Substituir regras de segurança para permitir atualizações de estado de controle de roteamento	Bool

Ações, recursos e chaves de condição do Amazon Route 53 Recovery Controls

O Amazon Route 53 Recovery Controls (prefixo do serviço: `route53-recovery-control-config`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Route 53 Recovery Controls
- Tipos de recursos definidos pelo Amazon Route 53 Recovery Controls
- Chaves de condição para o Amazon Route 53 Recovery Controls

Ações definidas pelo Amazon Route 53 Recovery Controls

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateCluster	Concede permissão para criar um cluster.	Gravar	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateControlPanel	Concede permissão para criar um painel de controle	Gravar	controlpanel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRoutingControl	Concede permissão para criar um controle de roteamento	Gravar	routingcontrol*		
CreateSafetyRule	Concede permissão para criar uma regra de segurança	Gravar	safetyrule*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteCluster	Concede permissão para excluir um cluster	Gravar	cluster*		
DeleteControlPanel	Concede permissão para descrever um painel de controle	Gravar	controlpanel*		
DeleteResourcePolicy [somente permissão]	Concede permissão para excluir a política de controle de acesso à RAM para um cluster	Gravar	cluster*		
DeleteRoutingControl	Concede permissão para excluir um controle de roteamento	Write	routingcontrol*		
DeleteSafetyRule	Concede permissão para excluir uma regra de segurança	Write	safetyrule*		
DescribeCluster	Concede permissão para descrever um cluster	Read	cluster*		
DescribeControlPanel	Concede permissão para descrever um painel de controle	Read	controlpanel*		
DescribeRoutingControl	Concede permissão para descrever um controle de roteamento	Read	routingcontrol*		
DescribeRoutingControlByName	Concede permissão para descrever um controle de roteamento	Read	routingcontrol*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeSafetyRule	Concede permissão para descrever uma regra de segurança	Leitura	safetyrule*		
GetResourcePolicy	Concede permissão para obter a política de recurso de um cluster	Leitura	cluster*		
ListAssociatedRoute53HealthChecks	Concede permissão para listar as verificações de integridade do Route 53 associadas	Lista			
ListClusters	Concede permissão para listar clusters	Leitura			
ListControlPanels	Concede permissão para listar painéis de controle	Read			
ListRoutingControls	Concede permissão para listar controles de roteamento	Leitura			
ListSafetyRules	Concede permissão para listar as regras de segurança	Leitura	controlpanel*		
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura			
PutResourcePolicy [somente permissão]	Concede permissão para definir a política de controle de acesso à RAM para um cluster	Gravar	cluster*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para marcar um recurso	Tags	cluster		
			controlpanel		
			safetyrule		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover etiquetas de um recurso	Tags	cluster		
			controlpanel		
			safetyrule		
				aws:TagKeys	
UpdateCluster	Concede permissão para atualizar um cluster	Gravar	cluster*		
UpdateControlPanel	Concede permissão para atualizar um cluster	Gravar	controlpanel*		
UpdateRoutingControl	Concede permissão para atualizar um controle de roteamento	Gravar	routingcontrol*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateSafetyRule	Concede permissão para atualizar uma regra de segurança	Gravar	safetyrule*		

Tipos de recursos definidos pelo Amazon Route 53 Recovery Controls

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
cluster	`arn:${Partition}:route53-recovery-control::${Account}:cluster/${ResourceId}`	aws:ResourceTag/${TagKey}
controlpanel	`arn:${Partition}:route53-recovery-control::${Account}:controlpanel/${ControlPanelId}`	aws:ResourceTag/${TagKey}
routingcontrol	`arn:${Partition}:route53-recovery-control::${Account}:controlpanel/${ControlPanelId}/routingcontrol/${RoutingControlId}`	
safetyrule	`arn:${Partition}:route53-recovery-control::${Account}:controlpanel/${Con`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
	`trolPanelId}/safetyrule/${SafetyRule Id}`	

Chaves de condição para o Amazon Route 53 Recovery Controls

O Amazon Route 53 Recovery Controls define as chaves de condição a seguir que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso pela chave e valor de uma etiqueta em uma solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o Amazon Route 53 Recovery Readiness

O Amazon Route 53 Recovery Readiness (prefixo do serviço: `route53-recovery-readiness`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Route 53 Recovery Readiness
- Tipos de recursos definidos pelo Amazon Route 53 Recovery Readiness
- Chaves de condição do Amazon Route 53 Recovery Readiness

Ações definidas pelo Amazon Route 53 Recovery Readiness

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de

condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateCell	Concede permissão para criar uma nova célula	Gravar	cell*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCrossAccountAuthorization	Concede permissão para criar uma autorização entre contas	Gravar			
CreateReadinessCheck	Concede permissão para criar uma verificação de preparação	Gravar	readinesscheck*		
				aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
CreateRecoveryGroup	Concede permissão para criar um grupo de recuperação	Gravar	recoverygroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateResourceSet	Concede permissão para criar um conjunto de recursos	Gravar	resourceset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCell	Concede permissão para excluir uma célula	Gravar	cell*		
DeleteCrossAccountAuthorization	Concede permissão para excluir uma autorização entre contas	Gravar			
DeleteReadinessCheck	Concede permissão para excluir uma verificação de preparação	Gravar	readinesscheck*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteRecoveryGroup	Concede permissão para excluir um grupo de recuperação	Gravar	recoverygroup*		
DeleteResourceSet	Concede permissão para excluir um conjunto de recursos	Gravar	resourceset*		
GetArchitectureRecommendations	Concede permissão para obter recomendações de arquitetura para um grupo de recuperação	Leitura	recoverygroup*		
GetCell	Concede permissão para obter informações sobre uma célula	Leitura	cell*		
GetCellReadinessSummary	Concede permissão para obter o resumo de preparação para uma célula	Leitura	cell*		
GetReadinessCheck	Concede permissão para obter informações sobre uma verificação de preparação	Leitura	readinesscheck*		
GetReadinessCheckResourceStatus	Concede permissão para obter o status de preparação de um recurso individual	Leitura	readinesscheck*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetReadinessCheckStatus	Concede permissão para obter o status de uma verificação de preparação (para um conjunto de recursos)	Leitura	readinesscheck*		
GetRecoveryGroup	Concede permissão para obter informações sobre um grupo de recuperação	Leitura	recoverygroup*		
GetRecoveryGroupReadinessSummary	Concede permissão para obter o resumo de preparação para um grupo de recuperação	Leitura	recoverygroup*		
GetResourceSet	Concede permissão para obter informações sobre um conjunto de recursos	Leitura	resourceset*		
ListCells	Concede permissão para listar células	Leitura			
ListCrossAccountAuthorizations	Concede permissão para listar autorizações entre contas	Leitura			
ListReadinessChecks	Concede permissão para listar verificações de preparação	Leitura			
ListRecoveryGroups	Concede permissão para listar grupos de recuperação	Leitura			
ListResourceSets	Concede permissão para listar conjuntos de recursos	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListRules	Concede permissão para listar regras de preparação	Read			
ListTagsForResources	Concede permissão para listar as etiquetas de um recurso	Read			
TagResource	Concede permissão para adicionar uma etiqueta a um recurso	Marcação	cell		
			readinesscheck		
			recoverygroup		
			resourceset		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover uma etiqueta de um recurso	Tags	cell		
			readinesscheck		
			recoverygroup		
			resourceset		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateCell	Concede permissão para atualizar uma célula	Gravar	cell*		
				aws:TagKeys	
UpdateReadinessCheck	Concede permissão para atualizar uma verificação de preparação	Gravar	readinesscheck*		
				aws:TagKeys	
UpdateRecoveryGroup	Concede permissão para atualizar um grupo de recuperação	Gravar	recoverygroup*		
				aws:TagKeys	
UpdateResourceSet	Concede permissão para atualizar um conjunto ed recursos	Gravar	resourceset*		
				aws:TagKeys	

Tipos de recursos definidos pelo Amazon Route 53 Recovery Readiness

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações

identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
readiness check	`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}
recoverygroup	`arn:${Partition}:route53-recovery-readiness::${Account}:recovery-group/${ResourceId}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Route 53 Recovery Readiness

O Amazon Route 53 Recovery Readiness define as chaves de condição a seguir que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Route 53 Resolver

O Amazon Route 53 Resolver (prefixo do serviço: `route53resolver`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Route 53 Resolver
- Tipos de recursos definidos pelo Amazon Route 53 Resolver
- Chaves de condição do Amazon Route 53 Resolver

Ações definidas pelo Amazon Route 53 Resolver

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou

ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateFirewallRuleGroup	Concede permissão para associar uma Amazon VPC a um grupo de regras de firewall especificado	Gravação	firewall-rule-group-association*		ec2:DescribeVpcs
				aws:RequestTag/${TagKey} aws:TagKeys	
AssociateResolverEndpointIpAddress	Concede permissão para associar um endereço IP especificado a um endpoint do Resolver. Este é um endereço IP pelo qual as consultas de DNS passam no caminho para sua rede (saída) ou sua VPCs (entrada)	Gravar	resolver-endpoint*		ec2:CreateNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets
AssociateResolverQueryLogConfig	Concede permissão para associar uma Amazon VPC a uma configuração de registro em log de consulta especificada	Gravação	resolver-query-log-config*		ec2:DescribeVpcs
AssociateResolverRule	Concede permissão para associar uma regra do	Gravação	resolver-rule*		ec2:DescribeVpcs

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	Resolver especificada a uma VPC especificada				
CreateFirewallDomainList	Concede permissão para criar uma lista de domínios do firewall.	Gravação	firewall-domain-list*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFirewallRule	Concede permissão para criar uma regra do firewall dentro de um grupo de regras do firewall.	Gravação	firewall-domain-list*		
			firewall-rule-group*		
CreateFirewallRuleGroup	Concede permissão para criar um grupo de regras do firewall.	Gravar	firewall-rule-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateOutpostResolver	Concede permissão para criar um Route 53 Resolver em Outposts	Gravar	outpost-resolver*		outposts:GetOutpost
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateResolverEndpoint	Concede permissão para criar um endpoint do Resolver. Há dois tipos de endpoints do Resolver, de entrada e de saída	Gravar	resolver-endpoint*		ec2:CreateNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateResolverQueryLogConfig	Concede permissão para criar uma configuração de registro de consultas do Resolver, que define onde você deseja que o Resolver salve os registros de consultas DNS que se originam em seu VPCs	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateResolverRule	Concede permissão para definir como rotear consultas originadas da VPC ou fora da VPC	Gravar	resolver-rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFirewallDomainList	Concede permissão para excluir uma lista de domínios do firewall.	Gravação	firewall-domain-list*		
DeleteFirewallRule	Concede permissão para excluir uma regra do firewall dentro de um grupo de regras do firewall.	Gravação	firewall-domain-list*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			firewall-rule-group*		
DeleteFirewallRuleGroup	Concede permissão para excluir um grupo de regras do firewall.	Gravar	firewall-rule-group*		
DeleteOutpostResolver	Concede permissão para excluir um Route 53 Resolver em Outposts	Gravar	outpost-resolver*		
DeleteResolverEndpoint	Concede permissão para excluir um endpoint do Resolver. O efeito de excluir um endpoint do Resolver depende do fato de ser um endpoint de entrada ou de saída	Gravação	resolver-endpoint*		ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces
DeleteResolverQueryLogConfig	Concede permissão para excluir uma configuração de registro log de consulta do Resolvedor	Gravação	resolver-query-log-config*		
DeleteResolverRule	Concede permissão para excluir uma regra do Resolver	Gravação	resolver-rule*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateFirewallRuleGroup	Concede permissão para remover a associação entre um grupo de regras do firewall especificado e uma VPC especificada	Gravação	firewall-rule-group-association*		
DisassociateResolverEndpointIpAddress	Concede permissão para remover um endereço IP especificado de um endpoint do Resolver. Este é um endereço IP pelo qual as consultas de DNS passam no caminho para sua rede (saída) ou sua VPCs (entrada)	Gravar	resolver-endpoint*		ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces
DisassociateResolverQueryLogConfig	Concede permissão para remover a associação entre uma configuração de registro em log de consulta do Resolver especificada e uma VPC especificada	Gravação	resolver-query-log-config*		
DisassociateResolverRule	Concede permissão para remover a associação entre uma regra do Resolver especificada e uma VPC especificada	Gravação	resolver-rule*		
GetFirewallConfig	Concede permissão para obter informações sobre uma configuração especificada do firewall.	Leitura	firewall-config*		ec2:DescribeVpcs

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetFirewallDomainList	Concede permissão para obter informações sobre uma lista de domínios do firewall especificada.	Leitura	firewall-domain-list*		
GetFirewallRuleGroup	Concede permissão para obter informações sobre um grupo de regras do firewall especificado.	Leitura	firewall-rule-group*		
GetFirewallRuleGroupAssociation	Concede permissão para obter informações sobre uma associação entre um grupo de regras do firewall especificado e uma VPC	Leitura	firewall-rule-group-association*		
GetFirewallRuleGroupPolicy	Concede permissão para obter informações sobre uma política de grupo de regras de Firewall especificada, que especifica as operações e os recursos do grupo de regras de Firewall que você deseja permitir que outra pessoa Conta da AWS use	Leitura	firewall-rule-group*		
GetOutpostResolver	Concede permissão para obter informações sobre um resolvedor do Route 53 especificado em Outposts	Leitura	outpost-resolver*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetResolverConfig	Concede permissão para obter o status do Resolver Config no recurso especificado	Leitura	resolver-config*		ec2:DescribeVpcs
GetResolverDnssecConfig	Concede permissão para obter o status de suporte de validação DNSSEC para consultas DNS dentro do recurso especificado	Leitura	resolver-dnssec-config*		
GetResolverEndpoint	Concede permissão para obter informações sobre um endpoint do Resolver especificado, por exemplo, se ele é um endpoint de entrada ou de saída, e os endereços IP na VPC para os quais as consultas de DNS são encaminhadas ao entrar ou sair da VPC	Leitura	resolver-endpoint*		
GetResolverQueryLogConfig	Concede permissão para obter informações sobre uma configuração específica de registro de consultas do Resolver, como o número da configuração para a VPCs qual a configuração está registrando consultas e o local para o qual os registros são enviados	Leitura	resolver-query-log-config*		ec2:DescribeVpcs

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetResolverQueryLogConfigAssociation	Concede permissão para obter informações sobre uma associação especificada entre uma configuração de registro em log de consulta do Resolver e uma Amazon VPC. Quando você associa uma VPC a uma configuração de registro em log de consulta, o Resolver registra consultas de DNS que se originam nessa VPC	Leitura			
GetResolverQueryLogConfigPolicy	Concede permissão para obter informações sobre uma política específica de registro de consultas do Resolver, que especifica as operações e os recursos de registro de consultas do Resolver que você deseja permitir que outra pessoa Conta da AWS use	Leitura	resolver-query-log-config*		
GetResolverRule	Concede permissão para obter informações sobre uma regra do Resolver especificada, como o nome do domínio para o qual a regra encaminha consultas de DNS e o endereço IP para o qual as consultas são encaminhadas.	Leitura	autodefined-rule resolver-rule		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetResolverRuleAssociation	Concede permissão para obter informações sobre uma associação entre uma regra do Resolver especificada e uma VPC	Leitura	autodefined-rule		
			resolver-rule		
GetResolverRulePolicy	Concede permissão para obter informações sobre uma política de regras do Resolver, que especifica as operações e os recursos do Resolver que você deseja permitir que outra pessoa Conta da AWS use	Leitura	resolver-rule*		
ImportFirewallDomains	Concede permissão para adicionar, remover ou substituir domínios do firewall em uma lista de domínios do firewall.	Gravar	firewall-domain-list*		
ListFirewallConfigs	Concede permissão para listar todas as configurações do Firewall que o current Conta da AWS é capaz de verificar	Lista			ec2:DescribeVpcs
ListFirewallDomainLists	Concede permissão para listar toda a lista de domínios do Firewall que Conta da AWS o atual é capaz de usar	Lista			
ListFirewallDomains	Concede permissão para listar todo o domínio do Firewall em uma lista de domínios do Firewall especificada	Lista	firewall-domain-list*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListFirewallRuleGroupAssociations	Concede permissão para listar informações sobre associações entre a Amazon VPCs e o grupo de regras do Firewall	Lista			
ListFirewallRuleGroups	Concede permissão para listar todo o grupo de regras do Firewall que Conta da AWS o atual é capaz de usar	Lista			
ListFirewallRules	Concede permissão para listar todas as regras de Firewall em um grupo de regras de Firewall especificado	Lista	firewall-rule-group*		
ListOutpostResolvers	Concede permissão para listar todas as instâncias do Route 53 Resolver em Outposts que foram criadas usando o atual Conta da AWS	Lista			
ListResolverConfigs	Concede permissão para listar os status do Resolver Config	Lista	resolver-config*		ec2:DescribeVpcs
ListResolverDnssecConfigs	Concede permissão para listar o status de suporte de validação DNSSEC para consultas DNS	Lista	resolver-dnssec-config*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListResolverEndpointIpAddresses	Concede permissão para listar os endereços IP pelos quais as consultas DNS passam no caminho para sua rede (saída) ou sua VPCs (entrada) para um endpoint específico do Resolver	Lista	resolver-endpoint*		
ListResolverEndpoints	Concede permissão para listar todos os endpoints do Resolver que foram criados usando o atual Conta da AWS	Lista			
ListResolverQueryLogConfigAssociations	Concede permissão para listar informações sobre associações entre a Amazon VPCs e as configurações de registro de consultas	Lista			ec2:DescribeVpcs
ListResolverQueryLogConfigs	Concede permissão para listar informações sobre as configurações de registro de consultas especificadas, que definem onde você deseja que o Resolver salve os registros de consultas de DNS e especifique VPCs aquelas para as quais você deseja registrar as consultas	Lista			ec2:DescribeVpcs

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListResolverRuleAssociations	Concede permissão para listar as associações que foram criadas entre as regras do Resolver e VPCs usando a atual Conta da AWS	Lista			ec2:DescribeVpcs
ListResolverRules	Concede permissão para listar as regras do Resolver que foram criadas usando o atual Conta da AWS	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas associadas ao recurso especificado	Leitura	firewall-domain-list		
			firewall-rule-group		
			firewall-rule-group-association		
			outpost-resolver		
			resolver-endpoint		
			resolver-query-log-config		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			resolver-rule		
PutFirewallRuleGroupPolicy	Concede permissão para especificar um Conta da AWS com o qual você deseja compartilhar um grupo de regras de Firewall, o grupo de regras de Firewall que você deseja compartilhar e as operações que você deseja que a conta possa realizar na configuração	Gerenciamento de permissões	firewall-rule-group*		
PutResolverQueryLogConfigPolicy	Concede permissão para especificar uma Conta da AWS com a qual você deseja compartilhar uma configuração de registro de consultas, a configuração de registro de consultas que você deseja compartilhar e as operações que você deseja que a conta possa realizar na configuração	Gerenciamento de permissões	resolver-query-log-config*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutResolverRulePolicy	Concede permissão para especificar uma Conta da AWS com a qual você deseja compartilhar regras, as regras do Resolver que você deseja compartilhar e as operações que você deseja que a conta possa realizar nessas regras	Gerenciamento de permissões	resolver-rule*		
TagResource	Concede permissão para adicionar uma ou mais etiquetas a um recurso especificado	Marcação	firewall-config		
			firewall-domain-list		
			firewall-rule-group		
			firewall-rule-group-association		
			outpost-resolver		
			resolver-dnssec-config		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			resolver-endpoint		
			resolver-query-log-config		
			resolver-rule		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover uma ou mais etiquetas de um recurso especificado	Marcação	firewall-config		
			firewall-domain-list		
			firewall-rule-group		
			firewall-rule-group-association		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			outpost-resolver		
			resolver-dnssec-config		
			resolver-endpoint		
			resolver-query-log-config		
			resolver-rule		
				aws:TagKeys	
UpdateFirewallConfig	Concede permissão para atualizar as definições selecionadas de uma configuração do firewall.	Gravação	firewall-config*		ec2:DescribeVpcs
UpdateFirewallDomains	Concede permissão para adicionar, remover ou substituir domínios do firewall em uma lista de domínios do firewall.	Gravação	firewall-domain-list*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateFirewallRule	Concede permissão para atualizar as configurações selecionadas de uma regra do firewall de um grupo de regras do firewall.	Gravação	firewall-domain-list*		
			firewall-rule-group*		
UpdateFirewallRuleGroupAssociation	Concede permissão para atualizar as configurações selecionadas de uma associação de grupo de regras do firewall.	Gravar	firewall-rule-group-association*		
UpdateOutpostResolver	Concede permissão para atualizar as configurações selecionadas para um Resolvedor da Rota 53 especificado em Outposts	Gravar	outpost-resolver*		
UpdateResolverConfig	Concede permissão para atualizar o status do Resolver Config no recurso especificado	Gravar	resolver-config*		ec2:DescribeVpcs
UpdateResolverDnssecConfig	Concede permissão para atualizar o status de suporte de validação DNSSEC para consultas DNS dentro do recurso especificado	Gravação	resolver-dnssec-config*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateResolverEndpoint	Concede permissão para atualizar as configurações selecionadas de um endpoint do Resolver de entrada ou de saída	Gravação	resolver-endpoint*		ec2:AssignIpv6Addresses ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:ModifyNetworkInterfaceAttribute ec2:UnassignIpv6Addresses
UpdateResolverRule	Concede permissão para atualizar as configurações de uma regra do Resolver especificada	Gravação	resolver-rule*		

Tipos de recursos definidos pelo Amazon Route 53 Resolver

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves

são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
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}

Chaves de condição do Amazon Route 53 Resolver

O Amazon Route 53 Resolver define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pela presença de pares chave-valor da etiqueta anexados ao recurso	Segmento
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon S3 Express

Amazon S3 Express (prefixo do serviço: `s3express`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon S3 Express
- Tipos de recursos definidos pelo Amazon S3 Express
- Chaves de condição do Amazon S3 Express

Ações definidas pelo Amazon S3 Express

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAccessPoint	Concede permissão para criar um novo ponto de acesso	Write	accesspoint*		
				s3express:DataAccessPointAccount s3express:DataAccessPointArn	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3express:AccessPointNetworkOrigin s3express:authType s3express:LocationName s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256 aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
CreateBucket	Concede permissão para criar um novo bucket	Gravar	bucket*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3express:authType s3express:LocationName s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256 aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSession	Concede permissão para criar token de sessão, que é usado para objetos APIs como PutObject, GetObject, etc	Gravar	bucket*		
			accesspoint	s3express:Permissions	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3express:authType s3express:ResourceAccount s3express:SessionMode s3express:signatureAge s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256 s3express:x-amz-server-side-encryption	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3express:x-amz-server-side-encryption-aws-kms-key-id s3express:AllAccessRestrictedToLocalZoneGroup s3express:Permissions	
DeleteAccessPoint	Concede permissão para excluir o ponto de acesso nomeado no URI	Write	accesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				content-sha256	
DeleteAccessPointPolicy	Concede permissão para excluir a política em um ponto de acesso especificado	Gerenciamento de permissões	accesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				content-sha256	
DeleteAccessPointScope	Concede permissão para excluir a configuração do escopo em um ponto de acesso especificado	Gerenciamento de permissões	accesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				content-sha256	
DeleteBucket	Concede permissão para excluir o bucket nomeado no URI	Write	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteBucketPolicy	Concede permissão para excluir a política em um bucket especificado	Gerenciamento de permissões	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
GetAccessPoint	Concede permissão para retornar informações de configuração sobre o ponto de acesso especificado	Leitura	accesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				content-sha256	
GetAccessPointPolicy	Concede permissão para retornar a política de ponto de acesso associada ao ponto de acesso especificado	Leitura	accesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				content-sha256	
GetAccessPointScope	Concede permissão para retornar a configuração do escopo associada ao ponto de acesso especificado	Leitura	accesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				content-sha256	
GetBucketPolicy	Concede permissão para retornar a política do bucket especificado	Leitura	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetEncryptionConfiguration	Concede permissão para retornar a configuração de criptografia padrão de um bucket de diretório	Leitura	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetLifecycleConfiguration	Concede permissão para retornar as informações de configuração do ciclo de vida definidas em um bucket de diretório	Leitura	bucket*	s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAccessPointsForDirectoryBuckets	Concede permissão para listar pontos de acesso	Lista		s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAllMyDirectoryBuckets	Concede permissão para listar todos os buckets de diretório de propriedade do remetente autenticado da solicitação	Lista		s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
ListTagsForResource	Concede permissão para listar todas as tags de um recurso específico	Lista	accesspoint bucket		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
PutAccessPointPolicy	Concede permissão para associar uma política de acesso a um ponto de acesso especificado	Gerenciamento de permissões	accesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutAccessPointScope	Concede permissão para associar um ponto de acesso a uma configuração de escopo de ponto de acesso especificada	Gerenciamento de permissões	accesspoint*		
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3express:x-amz-content-sha256	
PutBucketPolicy	Concede permissão para adicionar ou substituir uma política de bucket em um bucket	Gerenciamento de permissões	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutEncryptionConfiguration	Concede permissão para definir a configuração de criptografia para um bucket de diretório	Gravar	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutLifecycleConfiguration	Concede permissão para criar uma nova configuração de ciclo de vida para o bucket de diretórios ou substituir uma configuração de ciclo de vida existente	Gravar	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
TagResource	Concede permissão para criar uma nova tag definida pelo usuário ou atualizar uma tag existente	Tags	accesspoint		
			bucket		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256 aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover as tags definidas pelo usuário especificadas de um recurso do S3	Tags	accesspoint		
			bucket		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256 aws:TagKeys	

Tipos de recursos definidos pelo Amazon S3 Express

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
bucket	`arn:${Partition}:s3express:${Region}:${Account}:bucket/${BucketName}`	aws:ResourceTag/${TagKey} s3express:BucketTag/${TagKey}
accesspoint	`arn:${Partition}:s3express:${Region}:${Account}:accesspoint/${AccessPointName}`	aws:ResourceTag/${TagKey} s3express:AccessPointTag/${TagKey}

Chaves de condição do Amazon S3 Express

O Amazon S3 Express define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Chaves de condição	Descrição	Tipo
s3express:AccessPointNetworkOrigin	Filtra o acesso pela origem de rede (Internet ou VPC)	String
s3express:AccessPointTag/${TagKey}	Filtra o acesso por pares de chave-valor de tag anexados ao ponto de acesso	String
s3express:AllAccessRestrictedToLocalZoneGroup	Filtra o acesso por grupo (s) de borda de rede da Zona AWS Local fornecidos nesta chave de condição	String
s3express:BucketTag/${TagKey}	Filtra o acesso por pares de chave-valor de tag anexados ao bucket	String
s3express:DataAccessPointAccount	Filtra o acesso pelo ID da AWS conta que possui o ponto de acesso	String
s3express:DataAccessPointArn	Filtra o acesso pelo nome de recurso da Amazon (ARN) de um ponto de acesso	ARN
s3express:LocationName	Filtra o acesso por uma zona de disponibilidade específica ou ID de zona local	String
s3express:Permissions	Filtra o acesso pela permissão solicitada pela configuração do escopo do ponto de acesso, como GetObject, PutObject	ArrayOfString

Chaves de condição	Descrição	Tipo
s3express:ResourceAccount	Filtra o acesso pelo Conta da AWS ID do proprietário do recurso	String
s3express:SessionMode	Filtra o acesso pela permissão solicitada pela CreateSession API, como ReadOnly e ReadWrite	String
s3express:TlsVersion	Filtra o acesso pela versão TLS usada pelo cliente	Numeric
s3express:authType	Filtra o acesso por método de autenticação	String
s3express:signatureAge	Filtra o acesso pela idade em milissegundos da assinatura da solicitação	Numérico
s3express:signatureversion	Filtra o acesso pela versão de AWS assinatura usada na solicitação	String
s3express:x-amz-content-sha256	Filtra o acesso por conteúdo não assinado em seu bucket	String
s3express:x-amz-server-side-encryption	Filtra o acesso pela criptografia do lado do servidor	String
s3express:x-amz-server-side-encryption-aws-kms-key-id	Filtra o acesso pela chave AWS KMS gerenciada pelo cliente para criptografia do lado do servidor	ARN

Ações, recursos e chaves de condição do Amazon S3 Glacier

Amazon S3 Glacier (prefixo do serviço: `glacier`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon S3 Glacier
- Tipos de recursos definidos pelo Amazon S3 Glacier
- Chaves de condição do Amazon S3 Glacier

Ações definidas pelo Amazon S3 Glacier

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AbortMultipartUpload	Concede permissão para anular um carregamento fracionado, identificado pelo ID do carregamento	Gravar	vault*		
AbortVaultLock	Anula o processo de bloqueio do cofre se o Vault Lock não estiver no estado Locked (Bloqueado)	Gerenciamento de permissões	vault*		
AddTagsToVault	Concede permissão para adicionar as etiquetas especificadas a um cofre	Tags	vault*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
CompleteMultipartUpload	Concede permissão para concluir um processo de carregamento fracionado	Gravar	vault*		
CompleteVaultLock	Concede permissão para concluir o processo de bloqueio do cofre	Gerenciamento de permissões	vault*		
CreateVault	Concede permissão para criar um novo cofre com o nome especificado	Gravar	vault*		
DeleteArchive	Concede permissão para excluir um arquivo de um cofre	Gravar	vault*		
				glacier:ArchiveAgeInDays	
DeleteVault	Concede permissão para excluir um cofre	Gravar	vault*		
DeleteVaultAccessPolicy	Concede permissão para excluir a política de acesso associada ao cofre especificado	Gerenciamento de permissões	vault*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteVaultNotifications	Concede permissão para excluir a configuração de notificação definida para um cofre	Gravar	vault*		
DescribeJob	Concede permissão para obter informações sobre um trabalho iniciado anteriormente	Leitura	vault*		
DescribeVault	Concede permissão para obter informações sobre um cofre	Leitura	vault*		
GetDataRetrievalPolicy	Concede permissão para recuperar a política de registro de dados	Leitura			
GetJobOutput	Concede permissão para baixar a saída do trabalho especificado	Leitura	vault*		
GetVaultAccessPolicy	Concede permissão para recuperar o sub-recurso access-policy definido no cofre	Leitura	vault*		
GetVaultLock	Concede permissão para recuperar os atributos do sub-recurso lock-policy definidos no cofre especificado	Leitura	vault*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetVaultNotifications	Concede permissão para recuperar o sub-recurso notification-configuration definido no cofre	Leitura	vault*		
InitiateJob	Concede permissão para iniciar um trabalho do tipo especificado	Gravar	vault*		
				glacier:ArchiveAgeInDays	
InitiateMultipartUpload	Concede permissão para iniciar um carregamento fracionado	Gravar	vault*		
InitiateVaultLock	Concede permissão para iniciar o processo de bloqueio do cofre	Gerenciamento de permissões	vault*		
ListJobs	Concede permissão para listar os trabalhos de um cofre que estão em andamento e os trabalhos que foram concluídos recentemente	Lista	vault*		
ListMultipartUploads	Concede permissão para listar os carregamentos fracionados em andamento para um cofre especificado	Lista	vault*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListParts	Concede permissão para listar as partes de um arquivamento que foram carregadas para um carregamento fracionado específico	Lista	vault*		
ListProvisionedCapacity	Concede permissão para listar a capacidade provisionada para o especificado Conta da AWS	Lista			
ListTagsForVault	Concede permissão para listar todas as etiquetas anexadas a um cofre	Lista	vault*		
ListVaults	Concede permissão para listar todos os cofres	Lista			
PurchaseProvisionedCapacity	Concede permissão para comprar uma unidade de capacidade provisionada para um Conta da AWS	Gravar			
RemoveTagsFromVault	Concede permissão para remover uma ou mais etiquetas do conjunto de etiquetas anexado a um cofre	Tags	vault*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SetDataRetrievalPolicy	Concede permissão para definir e, em seguida, coloca em prática uma política de recuperação de dados na região especificada na solicitação PUT	Gerenciamento de permissões			
SetVaultAccessPolicy	Concede permissão para configurar uma política de acesso para um cofre; isso substituirá uma política existente	Gerenciamento de permissões	vault*		
SetVaultNotifications	Concede permissão para configurar notificações do cofre	Gravar	vault*		
UploadArchive	Concede permissão para carregar um arquivo no cofre	Gravar	vault*		
UploadMultipartPart	Concede permissão para carregar uma parte de um arquivo	Gravar	vault*		

Tipos de recursos definidos pelo Amazon S3 Glacier

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
vault	`arn:${Partition}:glacier:${Region}:${Account}:vaults/${VaultName}`	

Chaves de condição do Amazon S3 Glacier

O Amazon S3 Glacier define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString
glacier:ArchiveAgeInDays	Filtra o acesso pelo tempo em que um arquivo foi armazenado no cofre, em dias	String
glacier:ResourceTag/	Filtra o acesso por uma etiqueta definida pelo cliente	String

Ações, recursos e chaves de condição do Amazon S3 Object Lambda

O Amazon S3 Object Lambda (prefixo de serviço: `s3-object-lambda`) fornece os recursos, ações e chaves de contexto de condição específicos do serviço a seguir para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon S3 Object Lambda
- Tipos de recursos definidos pelo Amazon S3 Object Lambda
- Chaves de condição para Amazon S3 Object Lambda

Ações definidas pelo Amazon S3 Object Lambda

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AbortMultipartUpload	Concede permissão para anular um multipart upload	Write	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				lambda:TlsVersion	
DeleteObject	Concede permissão para remover a versão nula de um objeto e inserir um marcador de exclusão, que se torna a versão atual do objeto	Write	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
DeleteObjectTagging	Concede permissão para usar o sub-recurso de marcação para remover todo o conjunto de etiquetas do objeto especificado	Marcação	objectlambdaaccesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
DeleteObjectVersion	Concede permissão para remover uma versão específica de um objeto	Write	objectlambdaaccesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
DeleteObjectVersionTagging	Concede permissão para remover todo o conjunto de etiquetas para uma versão específica do objeto	Marcação	objectlambdaaccesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
GetObject	Concede permissão para recuperar objetos do Amazon S3	Read	objectlambdaaccesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectAcl	Concede permissão para retornar a lista de controle de acesso (ACL) de um objeto	Read	objectlambdaaccesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectLegalHold	Concede permissão para obter o status atual de retenção legal de um objeto	Read	objectlambdaaccesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectRetention	Concede permissão para recuperar as configurações de retenção de um objeto	Read	objectlambdaaccesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectTagging	Concede permissão para retornar o conjunto de etiquetas de um objeto	Read	objectlambdaaccesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectVersion	Concede permissão para recuperar uma versão específica de um objeto	Read	objectlambdaaccesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
GetObjectVersionAcl	Concede permissão para retornar a lista de controle de acesso (ACL) de uma versão específica de objeto	Read	objectlambdaaccesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
GetObjectVersionTagging	Concede permissão para retornar o conjunto de etiquetas para uma versão específica do objeto	Read	objectlambdaaccesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
ListBucket	Concede permissão para listar alguns ou todos os objetos em um bucket do Amazon S3 (até 1.000)	List	objectlambdaaccesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
ListBucketMultipartUploads	Concede permissão para listar multipart uploads em andamento	List	objectlambdaaccesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
ListBucketVersions	Concede permissão para listar metadados sobre todas as versões de objetos em um bucket do Amazon S3	List	objectlambdaaccesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
ListMultipartUploadParts	Concede permissão para listar as partes que foram carregadas para um multipart upload específico	List	objectlambdaaccesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObject	Concede permissão para adicionar um objeto a um bucket	Gravar	objectlambdaaccesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutObjectAcl	Concede permissão para definir as permissões de lista de controle de acesso (ACL) para objetos novos ou existentes em um bucket do S3	Gerenciamento de permissões	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectLegalHold	Concede permissão para aplicar uma configuração de retenção legal ao objeto especificado	Write	objectlambdaaccesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectRetention	Concede permissão para colocar uma configuração de retenção de objetos em um objeto	Write	objectlambdaaccesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectTagging	Concede permissão para definir o conjunto de etiquetas fornecido para um objeto que já existe em um bucket	Marcação	objectlambdaaccesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutObjectVersionAcl	Concede permissão para usar o sub-recurso acl para definir as permissões de lista de controle de acesso (ACL) para um objeto que já existe em um bucket	Permissions management	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
PutObjectVersionTagging	Concede permissão para definir o conjunto de etiquetas fornecido para uma versão específica de um objeto	Marcação	objectlambdaaccesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
RestoreObject	Concede permissão para restaurar uma cópia arquivada de um objeto novamente no Amazon S3	Gravar	objectlambdaaccesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
WriteGetObjectResponse	Concede permissão para fornecer dados para GetObject solicitações enviadas ao S3 Object Lambda	Gravar	objectlambdaaccesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	

Tipos de recursos definidos pelo Amazon S3 Object Lambda

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
objectlambdaaccesspoint	`arn:${Partition}:s3-object-lambda:${Region}:${Account}:accesspoint/${AccessPointName}`	

Chaves de condição para Amazon S3 Object Lambda

O Amazon S3 Object Lambda define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
s3-object-lambda:TlsVersion	Filtra o acesso pela versão TLS usada pelo cliente	Numeric
s3-object-lambda:authType	Filtra o acesso por método de autenticação	String
s3-object-lambda:signatureAge	Filtra o acesso pela idade em milissegundos da assinatura da solicitação	Numeric
s3-object-lambda:versionid	Filtra o acesso por uma versão de objeto específica	String

Ações, recursos e chaves de condição do Amazon S3 on Outposts

O Amazon S3 on Outposts (prefixo do serviço: `s3-outposts`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon S3 on Outposts
- Tipos de recursos definidos pelo Amazon S3 on Outposts
- Chaves de condição para o Amazon S3 on Outposts

Ações definidas pelo Amazon S3 on Outposts

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AbortMultipartUpload	Concede permissão para anular um multipart upload	Write	object*		
				s3-outposts:DataAccessPointArn s3-outposts:DataAccessPointAccount s3-outposts:AccessPointNetworkOrigin s3-outpos	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
CreateAccessPoint	Concede permissão para criar um novo ponto de acesso	Write	accesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:x-amz-content-sha256	
CreateBucket	Concede permissão para criar um novo bucket	Write	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
CreateEndpoint	Concede permissão para criar um novo endpoint	Write	endpoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteAccessPoint	Concede permissão para excluir o ponto de acesso nomeado no URI	Write	accesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:DataAccessPointArn s3-outposts:DataAccessPointAccount s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:x-amz-content-sha256	
DeleteAccessPointPolicy	Concede permissão para excluir a política em um ponto de acesso especificado	Permissions management	accesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:DataAccessPointArn s3-outposts:DataAccessPointAccount s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:x-amz-content-sha256	
DeleteBucket	Concede permissão para excluir o bucket nomeado no URI	Write	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteBucketPolicy	Concede permissão para excluir a política em um bucket especificado	Permissions management	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
DeleteEndpoint	Concede permissão para excluir o endpoint nomeado no URI	Write	endpoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteObject	Concede permissão para remover a versão nula de um objeto e inserir um marcador de exclusão, que se torna a versão atual do objeto	Write	object*		
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signat	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ureversion s3-outposts:x-amz-content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteObjectTagging	Concede permissão para usar o sub-recurso de marcação para remover todo o conjunto de etiquetas do objeto especificado	Marcação	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outpos	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
DeleteObjectVersion	Concede permissão para remover uma versão específica de um objeto	Write	object*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:versionid s3-outposts:x-amz-content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteObjectVersionTagging	Concede permissão para remover todo o conjunto de etiquetas para uma versão específica do objeto	Tags	object*		
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outpos	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ts:signatureAge s3-outposts:signatureversion s3-outposts:versionid s3-outposts:x-amz-content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAccessPoint	Concede permissão para retornar informações de configuração sobre o ponto de acesso especificado	Read		s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:x-amz-content-sha256	
GetAccessPointPolicy	Concede permissão para retornar a política de ponto de acesso associada ao ponto de acesso especificado	Read	accesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:x-amz-content-sha256	
GetBucket	Concede permissão para retornar a configuração de bucket associada a um bucket do Amazon S3	Read	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
GetBucketPolicy	Concede permissão para retornar a política do bucket especificado	Read	bucket*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetBucketTagging	Concede permissão para retornar o conjunto de etiquetas associado a um bucket do Amazon S3	Read	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetBucketVersioning	Concede permissão para retornar o estado de versionamento de um bucket do Amazon S3	Leitura	bucket*	s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetLifecycleConfiguration	Concede permissão para retornar as informações de configuração de ciclo de vida definidas em um bucket do Amazon S3	Read	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
GetObject	Concede permissão para recuperar objetos do Amazon S3	Read	object*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outposts:signatureAge	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
GetObjectTagging	Concede permissão para retornar o conjunto de etiquetas de um objeto	Read	object*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outposts:signatureAge	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
GetObjectVersion	Concede permissão para recuperar uma versão específica de um objeto	Leitura	object*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outposts:signatureAge	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:signatureversion s3-outposts:versionid s3-outposts:x-amz-content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetObjectVersionForReplication	Concede permissão para replicar objetos não criptografados e objetos criptografados com o SSE-KMS	Leitura	object*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetObjectVersionTagging	Concede permissão para retornar o conjunto de etiquetas para uma versão específica do objeto	Read	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outpos	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ts:signatureAge s3-outposts:signatureversion s3-outposts:versionid s3-outposts:x-amz-content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetReplicationConfiguration	Concede permissão para obter as informações de configuração de replicação definidas em um bucket do Amazon S3	Leitura	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAccessPoints	Concede permissão para listar pontos de acesso	List		s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
ListBucket	Concede permissão para listar alguns ou todos os objetos em um bucket do Amazon S3 (até 1.000)	List	accesspoint* bucket*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:delimiter s3-outposts:max-keys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:prefix s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
ListBucketMultipartUploads	Concede permissão para listar multipart uploads em andamento	List	accesspoint* bucket*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:x-amz-content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListBucketVersions	Concede permissão para listar metadados sobre todas as versões de objetos em um bucket do Amazon S3	Lista	bucket*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:delimiter s3-outpos	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ts:max-keys s3-outposts:prefix s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
ListEndpoints	Concede permissão para listar endpoints	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListMultipartUploadParts	Concede permissão para listar as partes que foram carregadas para um multipart upload específico	Lista	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signat	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ureversion s3-outposts:x-amz-content-sha256	
ListOutpostsWithS3	Concede permissão para listar Outposts com capacidade do S3	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListRegionalBuckets	Concede permissão para listar todos os buckets de propriedade do remetente autenticado da solicitação	Lista		s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
ListSharedEndpoints	Concede permissão para listar endpoints compartilhados	Lista			
PutAccessPointPolicy	Concede permissão para associar uma política de acesso a um ponto de acesso especificado	Permissions management	accesspoint*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:x-amz-content-sha256	
PutBucketPolicy	Concede permissão para adicionar ou substituir uma política de bucket em um bucket	Permissions management	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutBucketTagging	Concede permissão para adicionar um conjunto de etiquetas a um bucket existente do Amazon S3	Marcação	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutBucketVersioning	Concede permissão para definir o estado de versionamento de um bucket existente do Amazon S3	Gravar	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutLifecycleConfiguration	Concede permissão para criar uma configuração de ciclo de vida para o bucket ou substituir uma configuração de ciclo de vida existente	Write	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
PutObject	Concede permissão para adicionar um objeto a um bucket	Write	object*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:RequestObjectTag/<key> s3-outposts:RequestObjectTagKeys s3-outpos	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				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-	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				metadata-directive s3-outposts:x-amz-server-side-encryption s3-outposts:x-amz-storage-class	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutObjectAcl	Concede permissão para definir as permissões de lista de controle de acesso (ACL) para um objeto que já existe em um bucket	Permissions management	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outpos	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-acl s3-outposts:x-amz-content-sha256 s3-outposts:x-amz-storage-class	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutObjectTagging	Concede permissão para definir o conjunto de etiquetas fornecido para um objeto que já existe em um bucket	Tags	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:RequestObjectTag/<key>	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:RequestObjectTagKeys s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutObjectVersionTagging	Concede permissão para definir o conjunto de etiquetas fornecido para uma versão específica de um objeto	Marcação	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:RequestObjectTag/<key>	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:RequestObjectTagKeys s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:versionid s3-outposts:x-amz-content-sha256	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutReplicationConfiguration	Concede permissão para criar uma configuração de replicação ou substituir uma existente	Gravar	bucket*		iam:PassRole
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
ReplicateDelete	Concede permissão para replicar marcadores de exclusão no bucket de destino	Write	object*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
Replicate Object	Concede permissão para replicar objetos e etiquetas de objetos no bucket de destino	Write	object*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256 s3-outposts:x-amz-server-side-encryption	
Replicate Tags	Concede permissão para replicar etiquetas de objetos no bucket de destino	Tags	object*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Tipos de recursos definidos pelo Amazon S3 on Outposts

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}`	

Chaves de condição para o Amazon S3 on Outposts

O Amazon S3 on Outposts define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
s3-outposts:AccessPointNetworkOrigin	Filtra o acesso pela origem de rede (Internet ou VPC)	String

Chaves de condição	Descrição	Type
s3-outposts:DataAccessPointAccount	Filtra o acesso pelo ID da AWS conta que possui o ponto de acesso	String
s3-outposts:DataAccessPointArn	Filtra o acesso pelo nome de recurso da Amazon (ARN) de um ponto de acesso	ARN
s3-outposts:ExistingObjectTag/<key>	Filtra o acesso exigindo que uma etiqueta de objeto existente tenha uma chave e um valor da etiqueta específicos	String
s3-outposts:RequestObjectTag/<key>	Filtra o acesso restringindo as chaves da etiqueta e os valores permitidos em objetos	String
s3-outposts:RequestObjectTagKeys	Filtra o acesso restringindo as chaves da etiqueta permitidas em objetos	String
s3-outposts:authType	Filtra o acesso restringindo solicitações de entrada a um método de autenticação específico	String
s3-outposts:delimiter	Filtra o acesso exigindo o parâmetro delimitador	String
s3-outposts:max-keys	Filtra o acesso limitando o número máximo de chaves retornadas em uma solicitação ListBucket	Numérico
s3-outposts:prefix	Filtra o acesso pelo prefixo do nome da chave	String

Chaves de condição	Descrição	Type
s3-outposts:signatureAge	Filtra o acesso identificando a duração da validade de uma assinatura, em milissegundos, em uma solicitação autenticada	Numérico
s3-outposts:signatureversion	Filtra o acesso identificando a versão do AWS Signature que é compatível com solicitações autenticadas	String
s3-outposts:versionid	Filtra o acesso por uma versão de objeto específica	String
s3-outposts:x-amz-acl	Filtra o acesso exigindo o x-amz-acl cabeçalho com uma ACL predefinida específica em uma solicitação	String
s3-outposts:x-amz-content-sha256	Filtra o acesso ao não permitir conteúdo não assinado no bucket	String
s3-outposts:x-amz-copy-source	Filtra o acesso restringindo a origem da cópia a um bucket, prefixo ou objeto específico	String
s3-outposts:x-amz-metadata-directive	Filtra o acesso permitindo a imposição do comportamento de metadados do objeto (COPY ou REPLACE) quando os objetos são copiados	String
s3-outposts:x-amz-server-side-encryption	Filtra o acesso exigindo criptografia do lado do servidor	String
s3-outposts:x-amz-storage-class	Filtra o acesso por classe de armazenamento	String

Ações, recursos e chaves de condição para tabelas do Amazon S3

O Amazon S3 Tables (prefixo do serviço:`s3tables`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelas tabelas do Amazon S3
- Tipos de recursos definidos pelas tabelas do Amazon S3
- Chaves de condição para tabelas do Amazon S3

Ações definidas pelas tabelas do Amazon S3

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateNamespace	Concede permissão para criar um namespace	Gravar	TableBucket*		
CreateTable	Concede permissão para criar uma tabela	Gravar	TableBucket*		
				s3tables:namespace s3tables:SSEAlgorithm	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				s3tables:KMSKeyAr	
CreateTableBucket	Concede permissão para criar um repositório de tabelas	Gravar	TableBucket*		
				s3tables:SSEAlgorithm s3tables:KMSKeyAr	
DeleteNamespace	Concede permissão para excluir um namespace	Gravar	TableBucket*		
				s3tables:namespace	
DeleteTable	Concede permissão para excluir uma tabela	Gravar	Table*		
				s3tables:namespace s3tables:tableName	
DeleteTableBucket	Concede permissão para excluir um bucket de tabela	Gravar	TableBucket*		
DeleteTableBucketEncryption	Concede permissão para excluir a configuração de criptografia em um bucket de tabela	Gravar	TableBucket*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteTableBucketPolicy	Concede permissão para excluir uma política em um repositório de tabelas	Gerenciamento de permissões	TableBucket*		
DeleteTablePolicy	Concede permissão para excluir uma política em uma tabela	Gerenciamento de permissões	Table*		
				s3tables:namespace s3tables:tableName	
GetNamespace	Concede permissão para obter um namespace	Leitura	TableBucket*		
				s3tables:namespace	
GetTable	Concede permissão para recuperar uma tabela	Leitura	Table*		
				s3tables:namespace s3tables:tableName	
GetTableBucket	Concede permissão para recuperar um bucket de mesa	Leitura	TableBucket*		
GetTableBucketEncryption	Concede permissão para recuperar a configuração de criptografia em um bucket de tabela	Leitura	TableBucket*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetTableBucketMaintenanceConfiguration	Concede permissão para recuperar uma configuração de manutenção em um bucket de tabela	Leitura	TableBucket*		
GetTableBucketPolicy	Concede permissão para recuperar uma política em um balde de mesa	Leitura	TableBucket*		
GetTableData [somente permissão]	Concede permissão para ler metadados e objetos de dados de um endpoint de armazenamento de tabelas usando o S3 APIs	Leitura	Table*		
				s3tables:namespace s3tables:tableName	
GetTableEncryption	Concede permissão para recuperar a configuração de criptografia em uma tabela	Leitura	Table*		
				s3tables:namespace s3tables:tableName	
GetTableMaintenanceConfiguration	Concede permissão para recuperar uma configuração de manutenção em uma tabela	Leitura	Table*		
				s3tables:namespace s3tables:tableName	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetTableMaintenanceJobStatus	Concede permissão para recuperar o status dos trabalhos de manutenção em uma tabela	Leitura	Table*		
				s3tables:namespace s3tables:tableName	
GetTableMetadataLocation	Concede permissão para recuperar a localização dos metadados de uma tabela	Leitura	Table*		
				s3tables:namespace s3tables:tableName	
GetTablePolicy	Concede permissão para recuperar uma política em uma tabela	Leitura	Table*		
				s3tables:namespace s3tables:tableName	
ListNamespaces	Concede permissão para listar namespaces	Lista	TableBucket*		
ListTableBuckets	Concede permissão para listar compartimentos de mesa	Lista			
ListTables	Concede permissão para listar tabelas	Lista	TableBucket*		
				s3tables:namespace	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutTableBucketEncryption	Concede permissão para colocar ou substituir a configuração de criptografia em um bucket de tabela	Gravar	TableBucket*		
				s3tables:KMSKeyAr s3tables:SSEAlgorithm	
PutTableBucketMaintenanceConfiguration	Concede permissão para colocar uma configuração de manutenção em um balde de mesa	Gravar	TableBucket*		
PutTableBucketPolicy	Concede permissão para criar ou substituir uma política em um repositório de tabelas	Gerenciamento de permissões	TableBucket*		
PutTableData [somente permissão]	Concede permissão para gravar metadados e objetos de dados em um endpoint de armazenamento de tabelas usando o S3 APIs	Gravar	Table*		
				s3tables:namespace s3tables:tableName	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutTableEncryption [somente permissão]	Concede permissão para colocar a configuração de criptografia em uma tabela	Gravar	Table*		
				s3tables:namespace s3tables:SSEAlgorithm s3tables:KMSKeyAr	
PutTableMaintenanceConfiguration	Concede permissão para colocar uma configuração de manutenção em uma tabela	Gravar	Table*		
				s3tables:namespace s3tables:tableName	
PutTablePolicy	Concede permissão para criar ou substituir uma política em uma tabela	Gerenciamento de permissões	Table*		
				s3tables:namespace s3tables:tableName	
RenameTable	Concede permissão para renomear uma tabela ou mover uma tabela entre namespaces	Gravar	Table*		
				s3tables:namespace s3tables:tableName	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateTableMetadataLocation	Concede permissão para atualizar a localização dos metadados de uma tabela	Gravar	Table*		
				s3tables:namespace s3tables:tableName	

Tipos de recursos definidos pelas tabelas do Amazon S3

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
TableBucket	`arn:${Partition}:s3tables:${Region}:${Account}:bucket/${TableBucketName}`	
Table	`arn:${Partition}:s3tables:${Region}:${Account}:bucket/${TableBucketName}/table/${TableID}`	s3tables:namespace s3tables:tableName

Chaves de condição para tabelas do Amazon S3

As tabelas do Amazon S3 definem as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais

as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
s3tables: KMSKeyArn	Filtra o acesso pelo ARN da chave AWS KMS para a chave usada para criptografar uma tabela	ARN
s3tables: SSEAlgorithm	Filtra o acesso pelo algoritmo de criptografia do lado do servidor usado para criptografar uma tabela	String
s3tables: namespace	Filtra o acesso pelos namespaces criados no bucket da tabela	String
s3tables: tableName	Filtra o acesso pelo nome das tabelas no compartimento de tabelas	String

Ações, recursos e chaves de condição para Amazon S3 Vectors

O Amazon S3 Vectors (prefixo do serviço:`s3vectors`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelos vetores do Amazon S3
- Tipos de recursos definidos pelos vetores do Amazon S3
- Chaves de condição para vetores do Amazon S3

Ações definidas pelos vetores do Amazon S3

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateIndex	Concede permissão para criar um novo índice vetorial dentro de um intervalo vetorial especificado	Gravar	Index*		
CreateVectorBucket	Concede permissão para criar um novo bucket vetorial	Gravar	VectorBucket*		
				s3vectors:sseType s3vectors:kmsKeyArn	
DeleteIndex	Concede permissão para excluir um índice vetorial especificado	Gravar	Index*		
DeleteVectorBucket	Concede permissão para excluir um bucket vetorial especificado	Gravar	VectorBucket*		
DeleteVectorBucketPolicy	Concede permissão para excluir a política de recursos do IAM de um bucket vetorial especificado	Gerenciamento de permissões	VectorBucket*		
DeleteVectors	Concede permissão para excluir um lote de vetores de um índice vetorial especificado	Gravar	Index*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetIndex	Concede permissão para obter os atributos de um índice vetorial especificado	Leitura	Index*		
GetVectorBucket	Concede permissão para obter os atributos de um bucket vetorial especificado	Leitura	VectorBucket*		
GetVectorBucketPolicy	Concede permissão para obter a política de recursos do IAM para um bucket vetorial específico	Leitura	VectorBucket*		
GetVectors	Concede permissão para obter um lote de vetores por meio de suas chaves vetoriais	Leitura	Index*		
ListIndexes	Concede permissão para obter uma lista paginada de todos os índices em um bucket vetorial especificado	Lista	VectorBucket*		
ListVectorBuckets	Concede permissão para obter uma lista paginada de todos os compartimentos vetoriais na conta	Lista			
ListVectors	Concede permissão para obter uma lista paginada de todos os vetores em um índice vetorial especificado	Lista	Index*		s3vectors:GetVectors

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutVectorBucketPolicy	Concede permissão para adicionar uma política de recursos do IAM a um bucket vetorial especificado	Gerenciamento de permissões	VectorBucket*		
PutVectors	Concede permissão para adicionar um lote de vetores a um índice vetorial especificado	Gravar	Index*		
QueryVectors	Concede permissão para encontrar vizinhos mais próximos aproximados em um índice vetorial de pesquisa especificado para um determinado vetor de consulta	Leitura	Index*		s3vectors:GetVectors

Tipos de recursos definidos pelos vetores do Amazon S3

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
Index	`arn:${Partition}:s3vectors:${Region}:${Account}:bucket/${BucketName}/index/${IndexName}`	
VectorBucket	`arn:${Partition}:s3vectors:${Region}:${Account}:bucket/${BucketName}`	

Chaves de condição para vetores do Amazon S3

O Amazon S3 Vectors define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
s3vectors:kmsKeyArn	Filtra o acesso pelo ARN da chave AWS KMS para a chave usada para criptografar um bucket vetorial	ARN
s3vectors:sseType	Filtra o acesso por tipo de criptografia do lado do servidor	String

Ações, recursos e chaves de condição para o assistente de ciência SageMaker de dados da Amazon

O assistente de ciência de SageMaker dados da Amazon (prefixo do serviço:`sagemaker-data-science-assistant`) fornece os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo assistente de ciência SageMaker de dados da Amazon
- Tipos de recursos definidos pelo assistente de ciência SageMaker de dados da Amazon
- Chaves de condição para o assistente SageMaker de ciência de dados da Amazon

Ações definidas pelo assistente de ciência SageMaker de dados da Amazon

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de

condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SendConversation [somente permissão]	Concede permissão para iniciar uma conversa com o assistente SageMaker de ciência de dados	Gravar			

Tipos de recursos definidos pelo assistente de ciência SageMaker de dados da Amazon

O assistente SageMaker de ciência de dados da Amazon não suporta a especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para permitir o acesso ao assistente de ciência de SageMaker dados da Amazon, especifique `"Resource": "*"` em sua política.

Chaves de condição para o assistente SageMaker de ciência de dados da Amazon

SageMakerDataScienceAssistant não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de

contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para as capacidades SageMaker geoespaciais da Amazon

Os recursos SageMaker geoespaciais da Amazon (prefixo do serviço:`sagemaker-geospatial`) fornecem os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelas capacidades SageMaker geoespaciais da Amazon
- Tipos de recursos definidos pelas capacidades SageMaker geoespaciais da Amazon
- Chaves de condição para recursos SageMaker geoespaciais da Amazon

Ações definidas pelas capacidades SageMaker geoespaciais da Amazon

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos

("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteEarthObservationJob	Concede permissão à DeleteEarthObservationJob operação que exclui um trabalho existente de observação da Terra	Gravar	EarthObservationJob*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteVectorEnrichmentJob	Concede permissão à DeleteVectorEnrichmentJob operação que exclui um trabalho de enriquecimento vetorial existente	Gravar	VectorEnrichmentJob*		
				aws:ResourceTag/${TagKey}	
ExportEarthObservationJob	Concede permissão para copiar os resultados de um trabalho de observação de terra para um local do S3	Gravar	EarthObservationJob*		iam:PassRole
				aws:ResourceTag/${TagKey}	
ExportVectorEnrichmentJob	Concede permissão para copiar os resultados de um VectorEnrichmentJob para um local do S3	Gravar	VectorEnrichmentJob*		iam:PassRole
				aws:ResourceTag/${TagKey}	
GetEarthObservationJob	Concede permissão para retornar detalhes sobre o trabalho de observação de terra	Leitura	EarthObservationJob*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetRasterDataCollection	Concede permissão para retornar detalhes sobre a coleta de dados de rasterização	Leitura	RasterDataCollection*		
				aws:ResourceTag/${TagKey}	
GetTile	Concede permissão para obter o bloco de um trabalho de observação de terra	Leitura	EarthObservationJob*		iam:PassRole
GetVectorEnrichmentJob	Concede permissão para retornar detalhes sobre o trabalho de enriquecimento de vetores	Leitura	VectorEnrichmentJob*		
				aws:ResourceTag/${TagKey}	
ListEarthObservationJobs	Concede permissão para retornar uma matriz de trabalhos de observação de terra associados à conta atual	Lista			
ListRasterDataCollections	Concede permissão para retornar uma matriz de coleções de dados de rasterização associados ao nome do modelo fornecido	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão à tag de listas para um SageMaker recurso geoespacial	Lista	EarthObservationJob		
			RasterDataCollection		
			VectorEnrichmentJob		
				aws:ResourceTag/${TagKey}	
ListVectorEnrichmentJobs	Concede permissão para retornar uma matriz de trabalhos de enriquecimento de vetores associados à conta atual	Lista			
SearchRasterDataCollection	Concede permissão para consultar coleções de dados de rasterização	Leitura			
StartEarthObservationJob	Concede permissão para a StartEarthObservationJob operação que inicia um novo trabalho de observação da Terra em sua conta	Gravar	EarthObservationJob*		iam:PassRole sagemaker-geospatial:TagResource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
StartVectorEnrichmentJob	Concede permissão à StartVectorEnrichmentJob operação que inicia um novo trabalho de enriquecimento vetorial em sua conta	Gravar	VectorEnrichmentJob*		iam:PassRole sagemaker-geospatial:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
StopEarthObservationJob	Concede permissão para a StopEarthObservationJob operação que interrompe um trabalho existente de observação da Terra	Gravar	EarthObservationJob*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopVectorEnrichmentJob	Concede permissão à StopVectorEnrichmentJob operação que interrompe um trabalho de enriquecimento vetorial existente	Gravar	VectorEnrichmentJob*		
				aws:ResourceTag/${TagKey}	
TagResource	Concede permissão para marcar um recurso SageMaker geoespacial	Tags	EarthObservationJob		
			RasterDataCollection		
			VectorEnrichmentJob		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permissão para desmarcar um recurso SageMaker geoespacial	Tags	EarthObservationJob		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			RasterDataCollection		
			VectorEnrichmentJob		
				aws:TagKeys	

Tipos de recursos definidos pelas capacidades SageMaker geoespaciais da Amazon

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Tipos de recursos	ARN	Chaves de condição
VectorEnrichmentJob	`arn:${Partition}:sagemaker-geospatial:${Region}:${Account}:vector-enrichment-job/${JobID}`	aws:ResourceTag/${TagKey}

Chaves de condição para recursos SageMaker geoespaciais da Amazon

Os recursos SageMaker geoespaciais da Amazon definem as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para a Amazon SageMaker com MLflow

A Amazon SageMaker com MLflow (prefixo do serviço:`sagemaker-mlflow`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon SageMaker com MLflow
- Tipos de recursos definidos pela Amazon SageMaker com MLflow
- Chaves de condição para Amazon SageMaker com MLflow

Ações definidas pela Amazon SageMaker com MLflow

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AccessUI	Concede permissão para acessar a MLflow interface do usuário	Leitura			
CreateExperiment	Concede permissão para criar um MLflow experimento	Gravar	mlflow-tracking-server*		
CreateModelVersion	Concede permissão para criar uma versão de modelo	Gravar	mlflow-tracking-server*		
CreateRegisteredModel	Concede permissão para criar um modelo registrado	Gravar	mlflow-tracking-server*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateRun	Concede permissão para criar uma execução em um experimento	Gravar	mlflow-tracking-server*		
DeleteExperiment	Concede permissão para marcar um MLflow experimento para exclusão	Gravar	mlflow-tracking-server*		
DeleteLoggedModel	Concede permissão para excluir um modelo conectado MLflow	Gravar	mlflow-tracking-server*		
DeleteLoggedModelTag	Concede permissão para excluir uma tag para um modelo conectado MLflow	Gravar	mlflow-tracking-server*		
DeleteModelVersion	Concede permissão para excluir uma versão de modelo	Gravar	mlflow-tracking-server*		
DeleteModelVersionTag	Concede permissão para excluir uma tag de versão de modelo	Gravar	mlflow-tracking-server*		
DeleteRegisteredModel	Concede permissão para excluir um modelo registrado	Gravar	mlflow-tracking-server*		
DeleteRegisteredModelAlias	Concede permissão para excluir um alias de modelo registrado	Gravar	mlflow-tracking-server*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteRegisteredModelTag	Concede permissão para excluir uma tag de modelo registrada	Gravar	mlflow-tracking-server*		
DeleteRun	Concede permissão para marcar uma execução para exclusão	Gravar	mlflow-tracking-server*		
DeleteTag	Concede permissão para excluir uma tag em uma execução	Gravar	mlflow-tracking-server*		
DeleteTraceTag	Concede permissão para excluir uma tag de rastreamento no MLflow	Gravar	mlflow-tracking-server*		
DeleteTraces	Concede permissão para excluir traços em MLflow	Gravar	mlflow-tracking-server*		
EndTrace	Concede permissão para finalizar um rastreamento em MLflow	Gravar	mlflow-tracking-server*		
FinalizeLoggedModel	Concede permissão para definir o status de um modelo conectado MLflow	Gravar	mlflow-tracking-server*		
GetDownloadURIForModelVersionArtifacts	Concede permissão para obter um URI e baixar artefatos de modelo para uma versão específica do modelo	Leitura	mlflow-tracking-server*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetExperiment	Concede permissão para obter metadados para um experimento MLflow	Leitura	mlflow-tracking-server*		
GetExperimentByName	Concede permissão para obter metadados de um MLflow experimento pelo nome	Leitura	mlflow-tracking-server*		
GetLatestModelVersions	Concede permissão para obter as versões mais recentes do modelo	Lista	mlflow-tracking-server*		
GetLoggedModel	Concede permissão para obter um modelo conectado MLflow	Leitura	mlflow-tracking-server*		
GetMetricHistory	Concede permissão para obter uma lista de todos os valores da métrica especificada para determinada execução	Leitura	mlflow-tracking-server*		
GetModelVersion	Concede permissão para obter uma versão do modelo por nome e versão do modelo	Leitura	mlflow-tracking-server*		
GetModelVersionByAlias	Concede permissão para obter a versão do modelo por alias em MLflow	Leitura	mlflow-tracking-server*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetRegisteredModel	Concede permissão para obter um modelo registrado	Leitura	mlflow-tracking-server*		
GetRun	Concede permissão para obter metadados, métricas, parâmetros e tags para uma execução	Leitura	mlflow-tracking-server*		
GetTraceInfo	Concede permissão para obter informações sobre um rastreamento em MLflow	Leitura	mlflow-tracking-server*		
ListArtifacts	Concede permissão para listar artefatos de uma execução	Lista	mlflow-tracking-server*		
ListLoggedModelArtifacts	Concede permissão para listar artefatos de um modelo registrado no MLflow	Lista	mlflow-tracking-server*		
LogBatch	Concede permissão para registrar em log um lote de métricas, parâmetros e tags para uma execução	Gravar	mlflow-tracking-server*		
LogInputs	Concede permissão para registrar em log entradas de uma execução	Gravar	mlflow-tracking-server*		
LogLoggedModelParams	Concede permissão para registrar parâmetros para um modelo registrado no MLflow	Gravar	mlflow-tracking-server*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
LogMetric	Concede permissão para registrar em log uma métrica para uma execução	Gravar	mlflow-tracking-server*		
LogModel	Concede permissão para registrar em log o modelo associado a uma execução	Gravar	mlflow-tracking-server*		
LogOutputs	Concede permissão para registrar saídas, como modelos, para uma execução em MLflow	Gravar	mlflow-tracking-server*		
LogParam	Concede permissão para registrar em log um parâmetro rastreado durante uma execução	Gravar	mlflow-tracking-server*		
RenameRegisteredModel	Concede permissão para renomear um modelo registrado	Gravar	mlflow-tracking-server*		
RestoreExperiment	Concede permissão para restaurar um experimento marcado para exclusão	Gravar	mlflow-tracking-server*		
RestoreRun	Concede permissão para restaurar uma execução excluída	Gravar	mlflow-tracking-server*		
SearchExperiments	Concede permissão para pesquisar MLflow experimentos	Leitura	mlflow-tracking-server*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SearchLoggedModels	Concede permissão para pesquisar modelos registrados no MLflow	Leitura	mlflow-tracking-server*		
SearchModelVersions	Concede permissão para pesquisar uma versão do modelo	Leitura	mlflow-tracking-server*		
SearchRegisteredModels	Concede permissão para pesquisar modelos registrados em MLflow	Leitura	mlflow-tracking-server*		
SearchRuns	Concede permissão para pesquisar execuções que satisfaçam expressões	Leitura	mlflow-tracking-server*		
SearchTraces	Concede permissão para pesquisar traços em MLflow	Leitura	mlflow-tracking-server*		
SetExperimentTag	Concede permissão para definir uma tag em um experimento	Gravar	mlflow-tracking-server*		
SetLoggedModelTags	Concede permissão para definir tags para um modelo registrado no MLflow	Gravar	mlflow-tracking-server*		
SetModelVersionTag	Concede permissão para definir uma tag para a versão do modelo	Gravar	mlflow-tracking-server*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SetRegisteredModelAlias	Concede permissão para definir um alias de modelo registrado	Gravar	mlflow-tracking-server*		
SetRegisteredModelTag	Concede permissão para definir uma tag para um modelo registrado	Gravar	mlflow-tracking-server*		
SetTag	Concede permissão para definir uma tag em uma execução	Gravar	mlflow-tracking-server*		
SetTraceTag	Concede permissão para definir uma tag de rastreamento em MLflow	Gravar	mlflow-tracking-server*		
StartTrace	Concede permissão para iniciar um rastreamento em MLflow	Gravar	mlflow-tracking-server*		
TransitionModelVersionStage	Concede permissão para fazer a transição de uma versão do modelo para um estágio específico	Gravar	mlflow-tracking-server*		
UpdateExperiment	Concede permissão para atualizar os metadados de um experimento MLflow	Gravar	mlflow-tracking-server*		
UpdateModelVersion	Concede permissão para atualizar a versão do modelo	Gravar	mlflow-tracking-server*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateRegisteredModel	Concede permissão para atualizar um modelo registrado	Gravar	mlflow-tracking-server*		
UpdateRun	Concede permissão para atualizar metadados de execução	Gravar	mlflow-tracking-server*		

Tipos de recursos definidos pela Amazon SageMaker com MLflow

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
mlflow-tracking-server	`arn:${Partition}:sagemaker:${Region}:${Account}:mlflow-tracking-server/${MlflowTrackingServerName}`	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Chaves de condição para Amazon SageMaker com MLflow

A Amazon SageMaker com MLflow define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda

mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso por uma chave da etiqueta e par de valores	String
sagemaker:ResourceTag/${TagKey}	Filtra o acesso por uma chave da etiqueta e par de valores	String

Ações, recursos e chaves de condição do AWS Savings Plans

AWS O Savings Plans (prefixo do serviço:`savingsplans`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Savings Plans
- Tipos de recursos definidos pelo AWS Savings Plans
- Chaves de condição do AWS Savings Plans

Ações definidas pelo AWS Savings Plans

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSavingsPlan	Concede permissão para criar um savings plan	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteQueuedSavingsPlan	Concede permissão para excluir o savings plan em fila associado à conta de clientes	Write	savingsplan*		
				aws:ResourceTag/${TagKey}	
DescribeSavingsPlanRates	Concede permissão para descrever as taxas associadas ao savings plan dos clientes	Read	savingsplan*		
				aws:ResourceTag/${TagKey}	
DescribeSavingsPlans	Concede permissão para descrever os planos de economia associados à conta dos clientes	Read	savingsplan*		
				aws:ResourceTag/${TagKey}	
DescribeSavingsPlansOfferingRates	Concede permissão para descrever as taxas associadas a ofertas de planos de economia	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeSavingsPlansOfferings	Concede permissão para descrever as ofertas de planos de economia que o cliente está qualificado para comprar	Read			
ListTagsForResource	Concede permissão para listar as etiquetas de um savings plan	Lista	savingsplan*		
ReturnSavingsPlan	Concede permissão para retornar um Savings Plans	Gravar	savingsplan*		
				aws:ResourceTag/${TagKey}	
TagResource	Concede permissão para marcar um savings plan	Marcação	savingsplan*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para desmarcar um savings plan	Marcação	savingsplan*		
				aws:TagKeys	

Tipos de recursos definidos pelo AWS Savings Plans

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
savingsplan	`arn:${Partition}:savingsplans::${Account}:savingsplan/${ResourceId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Savings Plans

AWS O Savings Plans define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelo conjunto de valores permitido para cada uma das etiquetas	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelo valor-etiqueta associado ao recurso	String
aws:TagKeys	Filtra o acesso pela presença de etiquetas obrigatórias na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Secrets Manager

AWS O Secrets Manager (prefixo do serviço:`secretsmanager`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Secrets Manager
- Tipos de recursos definidos pelo AWS Secrets Manager
- Chaves de condição do AWS Secrets Manager

Ações definidas pelo AWS Secrets Manager

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchGetSecretValue	Concede permissão para recuperar e descriptografar uma lista de segredos	Lista			
CancelRotateSecret	Concede permissão para cancelar uma alternância do segredo em andamento	Gravar	Secret*		
				secretsmanager:SecretId secretsmanager:resource/All	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				owRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSecret	Concede permissão para criar um segredo que armazena dados criptografados que podem ser consultados e roteados	Gravar	Secret*	secretsmanager:Name secretsmanager:Description secretsmanager:KmsKeyArn secretsmanager:KmsKeyId aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys secretsmanager:ResourceTag/tag-key	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				secretsmanager:AddReplicaRegions secretsmanager:ForceOverwriteReplicaSecret	
DeleteResourcePolicy	Concede permissão para excluir a política de recursos anexada a um segredo	Gerenciamento de permissões	Secret*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
DeleteSecret	Concede permissão para excluir um segredo	Gravar	Secret*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:RecoveryWindowInDays secretsmanager:ForceDeleteWithoutRecovery secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:Sec	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				retPrimaryRegion	
DescribeSecret	Concede permissão para recuperar os metadados sobre um segredo, mas não os dados criptografados	Leitura	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
GetRandomPassword	Concede permissão para gerar uma string aleatória para uso na criação de senha	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetResourcePolicy	Concede permissão para obter a política de recursos anexada a um segredo	Leitura	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
GetSecretValue	Concede permissão para recuperar e descriptografar os dados criptografados	Leitura	Secret*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				secretsmanager:SecretId secretsmanager:VersionId secretsmanager:VersionStage secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListSecretVersionIds	Concede permissão para listar as versões disponíveis de um segredo	Leitura	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
ListSecrets	Concede permissão para listar os segredos disponíveis	Lista			
PutResourcePolicy	Concede permissão para anexar uma política de recursos a um segredo	Gerenciamento de permissões	Secret*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:BlockPublicPolicy secretsmanager:SecretPrimaryRegion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutSecretValue	Concede permissão para criar uma nova versão do segredo com novos dados criptografados	Gravar	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
RemoveRegionsFromReplication	Concede permissão para remover regiões da replicação	Gravar	Secret*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ReplicateSecretToRegions	Concede permissão para converter um segredo existente em um segredo multirregional e começa a replicá-lo a uma lista de novas regiões	Gravar	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:AddReplicaRegions secretsmanager:For	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ceOverwriteReplicaSecret	
RestoreSecret	Concede permissão para cancelar a exclusão de um segredo	Gravar	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
RotateSecret	Concede permissão para iniciar a alternância de um segredo	Gravar	Secret*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				secretsmanager:SecretId secretsmanager:RotationLambdaARN secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:Mod	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ifyRotationRules secretsmanager:RotateImmediately	
StopReplicationToReplica	Concede permissão para remover o segredo da replicação e promove o segredo para um segredo regional na Região da réplica	Gravar	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para adicionar etiquetas a um segredo	Tags	Secret*	secretsmanager:SecretId aws:RequestTag/${TagKey} aws:TagKeys secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para remover etiquetas de uma segredo	Tags	Secret*	secretsmanager:SecretId aws:TagKeys secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateSecret	Concede permissão para atualizar um segredo com novos metadados ou com uma nova versão dos dados criptografados	Gravar	Secret*	secretsmanager:SecretId secretsmanager:Description secretsmanager:KmsKeyArn secretsmanager:KmsKeyId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				secretsmanager:SecretPrimaryRegion	
UpdateSecretVersionStage	Concede permissão para mover um estágio de um segredo para outro	Gravar	Secret*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				secretsmanager:SecretId secretsmanager:VersionStage secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
ValidateResourcePolicy	Concede permissão para validar uma política de recursos antes de anexar a política	Gerenciamento de permissões	Secret*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Tipos de recursos definidos pelo AWS Secrets Manager

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves

são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
Secret	`arn:${Partition}:secretsmanager:${Region}:${Account}:secret:${SecretId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys secretsmanager:ResourceTag/tag-key secretsmanager:resource/AllowRotationLambdaArn

Chaves de condição do AWS Secrets Manager

AWS O Secrets Manager define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por uma chave que está presente na solicitação feita pelo usuário para o serviço Secrets Manager	String

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra o acesso por uma lista de todos os nomes de chaves de etiquetas presentes na solicitação feita pelo usuário para o serviço Secrets Manager	ArrayOfString
secretsmanager:AddReplicaRegions	Filtra o acesso pela lista de Regiões nas quais replicar o segredo	ArrayOfString
secretsmanager:BlockPublicPolicy	Filtra o acesso de acordo com o fato de a política de recursos bloquear o Conta da AWS acesso amplo	Bool
secretsmanager:Description	Filtra o acesso pelo texto da descrição na solicitação	String
secretsmanager:ForceDeleteWithoutRecovery	Filtra o acesso pela necessidade do segredo ser excluído imediatamente sem uma janela de recuperação	Bool
secretsmanager:ForceOverwriteReplicaSecret	Filtra o acesso por sobrescrever um segredo com o mesmo nome na Região de destino	Bool
secretsmanager:KmsKeyArn	Filtra o acesso pelo ARN da chave KMS na solicitação	ARN
secretsmanager:KmsKeyId	Filtra o acesso pelo identificador da chave KMS na solicitação. Obsoleto: use secretsmanager: KmsKeyArn	String

Chaves de condição	Descrição	Tipo
secretsmanager:ModifyRotationRules	Filtra o acesso de acordo com a necessidade de as regras de alternância do segredo serem modificadas	Bool
secretsmanager:Name	Filtra o acesso pelo nome amigável do segredo na solicitação	String
secretsmanager:RecoveryWindowInDays	Filtra o acesso pelo número de dias que o Secrets Manager aguarda antes de excluir o segredo	Numérico
secretsmanager:ResourceTag/tag-key	Filtra o acesso por uma chave da etiqueta e par de valores	String
secretsmanager:RotateImmediately	Filtra o acesso pela necessidade do segredo ser girado imediatamente	Bool
secretsmanager:RotationLambdaARN	Filtra o acesso pelo ARN da função de alternância do Lambda na solicitação	ARN
secretsmanager:SecretId	Filtra o acesso pelo valor de SecretID na solicitação	ARN
secretsmanager:SecretPrimaryRegion	Filtra o acesso por região primária na qual o segredo é criado se o segredo for um segredo multirregional	String
secretsmanager:VersionId	Filtra o acesso pelo identificador exclusivo da versão do segredo na solicitação	String

Chaves de condição	Descrição	Tipo
secretsmanager:VersionStage	Filtra o acesso pela lista de estágios de versão na solicitação	String
secretsmanager:resource/AllowRotationLambdaArn	Filtra o acesso pelo ARN da função de alternância do Lambda associada ao segredo	ARN

Ações, recursos e chaves de condição do AWS Security Hub

AWS O Security Hub (prefixo do serviço:`securityhub`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Security Hub
- Tipos de recursos definidos pelo AWS Security Hub
- Chaves de condição do AWS Security Hub

Ações definidas pelo AWS Security Hub

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptAdministratorInvitation	Concede permissão para aceitar convites do Security Hub para se tornar uma conta-membro	Write	hub		
AcceptInvitation	Concede permissão para aceitar convites do Security Hub para se tornar uma conta-membro	Gravar	hub		
BatchDeleteAutomationRules	Concede permissão para excluir uma ou mais regras de automação no Security Hub	Gravar	automation-rule*		
BatchDisableStandards	Concede permissão para desabilitar padrões no Security Hub	Write	hub		
BatchEnableStandards	Concede permissão para habilitar padrões no Security Hub	Gravar	hub		
BatchGetAutomationRules	Concede permissão para recuperar uma lista de detalhes das regras de automação do Security Hub com base na regra Amazon Resource Names () ARNs	Leitura	automation-rule*		
BatchGetConfigurationPolicyAssociations	Concede permissão para recuperar informações sobre políticas de configuração associadas a uma lista	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	específica de contas membros e unidades organizacionais da organização da conta chamadora				
BatchGetControlEvaluations [somente permissão]	Concede permissão para obter o status de habilitação e conformidade dos controles, a contagem de descobertas para os controles e a pontuação geral de segurança dos controles no console do Security Hub	Leitura	hub		
BatchGetSecurityControls	Concede permissão para obter detalhes sobre controles de segurança específicos identificados pelo ID ou ARN	Leitura			securityhub:DescribeStandardsControls
BatchGetStandardsControlAssociations	Concede permissão para obter o status de habilitação de um lote de controles de segurança em padrões	Leitura			securityhub:DescribeStandardsControls
BatchImportFindings	Concede permissão para importar descobertas para o Security Hub de um produto integrado	Gravar	product*		
				securityhub:TargetAccount	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchUpdateAutomationRules	Concede permissão para atualizar uma ou mais regras de automação do Security Hub com base na regra Amazon Resource Names (ARNs) e nos parâmetros de entrada	Gravar	automation-rule*		
BatchUpdateFindings	Concede permissão para atualizar campos controlados pelo cliente para um conjunto selecionado de descobertas do Security Hub	Gravar	hub		
			hubv2		
				securityhub:ASFFSyntaxPath/${ASFFSyntaxPath} securityhub:OCSFSyntaxPath/${OCSFSyntaxPath}	
BatchUpdateStandardsControlAssociations	Concede permissão para atualizar o status de habilitação de um lote de controles de segurança em padrões	Gravar			securityhub:UpdateStandardsControl

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ConnectorRegistrationsV2	Concede permissão para concluir o fluxo de código de autorização OAuth 2.0 com base nos parâmetros de entrada	Gravar			
CreateActionTarget	Concede permissão para criar ações personalizadas no Security Hub	Gravar	hub		
CreateAggregatorV2	Concede permissão para criar um AggregatorV2, que configura a agregação de dados entre regiões	Gravar			
CreateAutomationRule	Concede permissão para criar uma regra de automação com base nos parâmetros de entrada	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAutomationRuleV2	Concede permissão para criar uma regra de automação V2 com base nos parâmetros de entrada	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateConfigurationPolicy	Concede permissão para criar uma política de configuração para gerenciar as configurações dos membros da organização no Security Hub	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnectorV2	Concede permissão para criar um conector V2 com base nos parâmetros de entrada	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFindingAggregator	Concede permissão para criar um agregador de descoberta, que contém a configuração de agregação de localização entre Regiões	Gravar			
CreateInsight	Concede permissão para criar insights no Security Hub. Insights são coleções de descobertas relacionadas	Write	hub		
CreateMembers	Concede permissão para criar contas-membro no Security Hub	Gravar	hub		
CreateTicketV2	Concede permissão para criar um ticket para uma descoberta do OCSF selecionada	Gravar	connectorv2		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeclineInvitations	Concede permissão para recusar convites do Security Hub para se tornar uma conta-membro	Write	hub		
DeleteActionTarget	Concede permissão para excluir ações personalizadas no Security Hub	Gravar	hub		
DeleteAggregatorV2	Concede permissão para excluir um AggregatorV2, que configura a agregação de dados entre regiões	Gravar	aggregatorv2*		
DeleteAutomationRuleV2	Concede permissão para excluir uma regra de automação V2 no Security Hub	Gravar	automation-rulev2*		
DeleteConfigurationPolicy	Concede permissão para excluir uma política de configuração existente	Gravar	configuration-policy*		
DeleteConnectorV2	Concede permissão para excluir um conector V2 no Security Hub	Gravar	connectorv2*		
DeleteFindingAggregator	Concede permissão para excluir um agregador de descoberta, o que desabilita a encontrar agregação entre Regiões	Gravar	finding-aggregator*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteInsight	Concede permissão para excluir insights do Security Hub	Write	hub		
DeleteInvitations	Concede permissão para excluir convites do Security Hub para se tornar uma conta-membro	Write	hub		
DeleteMembers	Concede permissão para excluir contas-membro do Security Hub	Write	hub		
DescribeActionTargets	Concede permissão para recuperar uma lista de ações personalizadas usando a API	Read	hub		
DescribeHub	Concede permissão para recuperar informações sobre o recurso do hub em sua conta	Read	hub		
DescribeOrganizationConfiguration	Concede permissão para descrever a configuração da organização para o Security Hub	Read	hub		
DescribeProducts	Concede permissão para recuperar informações sobre as integrações de produtos do Security Hub disponíveis	Leitura	hub		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeProductsV2	Concede permissão para recuperar informações sobre as integrações de produtos do Security Hub V2 disponíveis	Leitura	hubv2		
DescribeSecurityHubV2	Concede permissão para recuperar informações sobre o recurso hub V2 em sua conta	Leitura			
DescribeStandards	Concede permissão para recuperar informações sobre padrões do Security Hub	Read	hub		
DescribeStandardsControls	Concede permissão para recuperar informações sobre controles de padrões do Security Hub	Read	hub		
DisableImportFindingsForProduct	Concede permissão para desabilitar a importação de descobertas de um produto integrado do Security Hub	Write	hub		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisableOrganizationAdminAccount	Concede permissão para remover a conta de administrador do Security Hub de sua organização	Write	hub		organizations:DeregisterDelegatedAdministrator organizations:DescribeOrganization organizations:ListDelegatedAdministrators
DisableSecurityHub	Concede permissão para desabilitar o Security Hub	Gravar	hub		
DisableSecurityHubV2	Concede permissão para desativar o Security Hub V2	Gravar			
DisassociateFromAdministratorAccount	Concede permissão a uma conta de membro do Security Hub para se desassociar da conta de administrador associada	Write	hub		
DisassociateFromMasterAccount	Concede permissão a uma conta-membro do Security Hub para desassociá-la da conta mestra associada	Write	hub		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateMembers	Concede permissão para desassociar contas de membros do Security Hub da conta de administrador associada	Write	hub		
EnableImportFindingsForProduct	Concede permissão para habilitar a importação de descobertas de um produto integrado do Security Hub	Write	hub		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
EnableOrganizationAdminAccount	Concede permissão para designar uma conta de administrador do Security Hub para sua organização	Write	hub		organizations:DescribeOrganization organizations:EnableAWSServiceAccess organizations:ListAWSServiceAccessForOrganization organizations:ListDelegatedAdministrators organizations:RegisterDelegatedAdministrator
EnableSecurityHub	Concede permissão para habilitar o Security Hub	Gravar	hub		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
EnableSecurityHubV2	Concede permissão para habilitar o Security Hub V2	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
GetAdhocInsightResults [somente permissão]	Concede permissão para recuperar dados estatísticos agregados sobre as descobertas	Leitura	hub hubv2		
GetAdministratorAccount	Concede permissão para recuperar detalhes sobre a conta de administrador do Security Hub	Leitura	hub		
GetAggregatorV2	Concede permissão para recuperar detalhes de um AggregatorV2, que configura a agregação de dados entre regiões	Leitura	aggregatorv2*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAutomationRuleV2	Concede permissão para recuperar detalhes de uma regra de automação V2 do Security Hub com base na regra Amazon Resource Name (ARN)	Leitura	automation-rulev2*		
GetConfigurationPolicy	Concede permissão para obter uma visão geral completa de uma política de configuração criada pela conta chamadora	Leitura	configuration-policy*		
GetConfigurationPolicyAssociation	Concede permissão para recuperar informações sobre uma política de configuração associada a uma conta membro ou unidade organizacional da organização da conta chamadora	Leitura			
GetConnectorV2	Concede permissão para recuperar detalhes de um conector V2 do Security Hub com base no ID do conector	Leitura	connectorv2*		
GetControlFindingSummary [somente permissão]	Concede permissão para recuperar uma pontuação de segurança e contagens de status de localização e controle de um padrão de segurança	Read	hub		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetEnabledStandards	Concede permissão para recuperar uma lista dos padrões que estão habilitados no Security Hub	Lista	hub		
GetFindingAggregator	Concede permissão para recuperar detalhes de um agregador de descoberta, que configura a agregação de localização entre Regiões	Leitura	finding-aggregator*		
GetFindingHistory	Concede permissão para recuperar uma lista de histórico de descobertas do Security Hub	Leitura	hub		
GetFindings	Concede permissão para recuperar uma lista de descobertas do Security Hub	Read	hub		
			hubv2		
GetFreeTrialEndDate [somente permissão]	Concede permissão para recuperar a data de término da avaliação gratuita de uma conta do Security Hub	Read	hub		
GetFreeTrialUsage [somente permissão]	Concede permissão para recuperar informações sobre o uso do Security Hub durante o período de avaliação gratuita	Read	hub		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetInsightFindingTrend [somente permissão]	Concede permissão para recuperar uma tendência de descoberta de insights do Security Hub para gerar um gráfico	Read	hub		
GetInsightResults	Concede permissão para recuperar resultados de insights do Security Hub	Read	hub		
GetInsights	Concede permissão para recuperar insights do Security Hub	List	hub		
GetInvitationsCount	Concede permissão para recuperar a conetiquetaem de convites de associação do Security Hub enviados para a conta	Read	hub		
GetMasterAccount	Concede permissão para recuperar detalhes sobre a conta mestra do Security Hub	Read	hub		
GetMembers	Concede permissão para recuperar os detalhes das contas-membro do Security Hub	Leitura	hub		
GetResourcesStatisticsV2	Concede permissão para recuperar estatísticas agregadas sobre recursos	Leitura	hubv2		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetResourcesV2	Concede permissão para recuperar uma lista de recursos	Leitura	hubv2		
GetSecurityControlDefinition	Concede permissão para obter os detalhes de definição de um controle de segurança específico identificados por ID	Leitura			securityhub:DescribeStandardsControls
GetUsage [somente permissão]	Concede permissão para recuperar informações sobre o uso do Security Hub por contas	Leitura	hub		
InviteMembers	Concede permissão para convidar outras AWS contas para se tornarem contas membros do Security Hub	Gravar	hub		
ListAggregatorsV2	Concede permissão para recuperar uma lista de AggregatorsV2, que configura a agregação de dados entre regiões	Lista			
ListAutomationRules	Concede permissão para recuperar uma lista de regras de automação e seus metadados da conta de chamada do Security Hub	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAutomationRulesV2	Concede permissão para recuperar uma lista de regras de automação V2 e seus metadados para a conta de chamada do Security Hub	Lista			
ListConfigurationPolicies	Concede permissão para listar os resumos de todas as políticas de configuração criadas pela conta chamadora	Lista			
ListConfigurationPolicyAssociations	Concede permissão para recuperar informações sobre todas as políticas de configuração associadas a todas as contas membros e unidades organizacionais da organização da conta chamadora	Lista			
ListConnectorsV2	Concede permissão para recuperar uma lista de conectores V2 e seus metadados para a conta de chamada do Security Hub	Lista			
ListControlEvaluationSummaries [somente permissão]	Concede permissão para recuperar uma lista de controles para um padrão, incluindo o controle IDs, os status e as contagens de descobertas	Leitura	hub		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListEnabledProductsForImport	Concede permissão para recuperar os produtos integrados do Security Hub que estão habilitados no momento	Lista	hub		
ListFindingAggregators	Concede permissão para recuperar uma lista de agregadores de localização, que contêm a configuração de agregação de descoberta entre Regiões	Lista			
ListInvitations	Concede permissão para recuperar os convites do Security Hub enviados para a conta	List	hub		
ListMembers	Concede permissão para recuperar detalhes sobre contas de membros do Security Hub associadas à conta de administrador	List	hub		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListOrganizationAdminAccounts	Concede permissão para listar as contas de administrador do Security Hub para sua organização	Lista	hub		organizations:DescribeOrganization organizations:ListDelegatedAdministrators
ListSecurityControlDefinitions	Concede permissão para recuperar uma lista de definições de controle de segurança, que contêm detalhes para controles de segurança na região atual	Lista			
ListStandardsControlAssociations	Concede permissão para listar o status de habilitação de um controle de segurança em padrões	Lista			securityhub:DescribeStandardsControls
ListTagsForResource	Concede permissão para listar as etiquetas associadas a um recurso	Read	automation-rule		
			configuration-policy		
			hub		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SendFindingEvents [somente permissão]	Concede permissão para usar uma ação personalizada para enviar descobertas do Security Hub para a Amazon EventBridge	Leitura	hub		
SendInsightEvents [somente permissão]	Concede permissão para usar uma ação personalizada para enviar insights do Security Hub para a Amazon EventBridge	Leitura	hub		
StartConfigurationPolicyAssociation	Concede permissão para associar uma política de configuração a uma conta membro ou unidade organizacional na organização da conta chamadora	Gravar	configuration-policy		
StartConfigurationPolicyDisassociation	Concede permissão para remover uma associação de política de configuração de uma conta membro ou unidade organizacional na organização da conta chamadora	Gravar	configuration-policy		
TagResource	Concede permissão para adicionar etiquetas a um recurso do Security Hub	Marcação	aggregatorv2		
			automation-rule		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			automation-rulev2		
			configuration-policy		
			connectorv2		
			hub		
			hubv2		
UntagResource	Concede permissão para remover etiquetas de um recurso do Security Hub	Marcação	aggregatorv2		
			automation-rule		
			automation-rulev2		
			configuration-policy		
			connectorv2		
			hub		
			hubv2		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateActionTarget	Concede permissão para atualizar ações personalizadas no Security Hub	Gravar	hub		
UpdateAggregatorV2	Concede permissão para atualizar um AggregatorV2, que configura a agregação de dados entre regiões	Gravar	aggregatorv2*		
UpdateAutomationRuleV2	Concede permissão para atualizar uma regra de automação V2 no Security Hub com base na regra Amazon Resource Name (ARN) e nos parâmetros de entrada	Gravar	automation-rulev2*		
UpdateConfigurationPolicy	Concede permissão para atualizar uma política de configuração existente	Gravar	configuration-policy*		
UpdateConnectorV2	Concede permissão para atualizar um conector V2 no Security Hub com base no ID do conector e nos parâmetros de entrada	Gravar	connectorv2*		
UpdateFindingAggregator	Concede permissão para atualizar um agregador de descoberta, que contém a configuração de agregação de localização entre Regiões	Gravar	finding-aggregator*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateFindings	Concede permissão para atualizar as descobertas do Security Hub	Write	hub		
UpdateInsight	Concede permissão para atualizar insights no Security Hub	Write	hub		
UpdateOrganizationConfiguration	Concede permissão para atualizar a configuração da organização para o Security Hub	Gravar	hub		
UpdateSecurityControl	Concede permissão para atualizar propriedades de um controle de segurança específico identificado por ID ou ARN	Gravar			securityhub:UpdateStandardsControl
UpdateSecurityHubConfiguration	Concede permissão para atualizar a configuração do Security Hub	Write	hub		
UpdateStandardsControl	Concede permissão para atualizar os controles de padrões do Security Hub	Write	hub		

Tipos de recursos definidos pelo AWS Security Hub

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves

são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
hub	arn:${Partition}:securityhub:${Region}:${Account}:hub/default	aws:ResourceTag/${TagKey}
hubv2	arn:${Partition}:securityhub:${Region}:${Account}:hubv2/${HubV2Id}	aws:ResourceTag/${TagKey}
product	arn:${Partition}:securityhub:${Region}:${Account}:product/${Company}/${ProductId}	
finding-aggregator	arn:${Partition}:securityhub:${Region}:${Account}:finding-aggregator/${FindingAggregatorId}	
aggregatorv2	arn:${Partition}:securityhub:${Region}:${Account}:aggregatorv2/${AggregatorV2Id}	aws:ResourceTag/${TagKey}
automation-rule	arn:${Partition}:securityhub:${Region}:${Account}:automation-rule/${AutomationRuleId}	aws:ResourceTag/${TagKey}
automation-rulev2	arn:${Partition}:securityhub:${Region}:${Account}:automation-rulev2/${AutomationRuleV2Id}	aws:ResourceTag/${TagKey}
configuration-policy	arn:${Partition}:securityhub:${Region}:${Account}:configuration-policy/${ConfigurationPolicyId}	aws:ResourceTag/${TagKey}
connectorv2	arn:${Partition}:securityhub:${Region}:${Account}:connectorv2/${ConnectorV2Id}	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Security Hub

AWS O Security Hub define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por ações com base na presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por ações com base nos pares de chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso por ações com base na presença de chaves da etiqueta na solicitação	ArrayOfString
securityhub:ASFFSyntaxPath/${ASFFSyntaxPath}	Filtra o acesso pelos campos e valores especificados na solicitação	String
securityhub:OCSFSyntaxPath/${OCSFSyntaxPath}	Filtra o acesso pelos campos e valores especificados na solicitação	String
securityhub:TargetAccount	Filtra o acesso pelo AwsAccountId campo especificado na solicitação	String

Ações, recursos e chaves de condição para Resposta a Incidentes AWS de Segurança

AWS O Security Incident Response (prefixo do serviço:`security-ir`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Resposta a Incidentes de AWS Segurança
- Tipos de recursos definidos pelo AWS Security Incident Response
- Chaves de condição para resposta a incidentes de AWS segurança

Ações definidas pela Resposta a Incidentes de AWS Segurança

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar

a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchGetMemberAccountDetails	Concede permissão para obter detalhes da conta do membro em lote	Leitura	membership*		
CancelMembership	Concede permissão para cancelar uma associação	Gravar	membership*		
CloseCase	Concede permissão para encerrar um caso	Gravar	case*		
CreateCase	Concede permissão para criar um caso	Gravar	case*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCaseComment	Concede permissão para criar um comentário de caso	Gravar	case*		
CreateMembership	Concede permissão para criar uma associação	Gravar	membership*		iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:ListDelegatedAdministrators
				aws:RequestTag/${TagKey} aws:TagKeys	
GetCase	Concede permissão para obter um caso	Leitura	case*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetCaseAttachmentDownloadUrl	Concede permissão para obter o URL de download do anexo do caso	Leitura	case*		
GetCaseAttachmentUploadUrl	Concede permissão para obter o URL de upload de um anexo de caso	Gravar	case*		
GetMembership	Concede permissão para se tornar membro	Leitura	membership*		
ListCaseEdits	Concede permissão para listar edições de casos	Leitura	case*		
ListCases	Concede permissão para listar casos	Lista			
ListComments	Concede permissão para listar comentários de casos	Leitura	case*		
ListMemberships	Concede permissão para listar associações	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas anexadas ao recurso especificado	Leitura	case		
			membership		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para adicionar tags ao recurso especificado	Tags	case		
			membership		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover tags do recurso especificado	Tags	case		
			membership		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCase	Concede permissão para atualizar um caso	Gravar	case*		
UpdateCaseComment	Concede permissão para atualizar um comentário de caso	Gravar	case*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateCaseStatus	Concede permissão para atualizar o status de um caso	Gravar	case*		
UpdateMembership	Concede permissão para atualizar associações	Gravar	membership*		iam:CreateServiceLinkedRole organizations:DescribeOrganizationalUnit
UpdateResolverType	Concede permissão para atualizar o tipo de resolvedor de casos	Gravar	case*		

Tipos de recursos definidos pelo AWS Security Incident Response

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
case	`arn:${Partition}:security-ir:${Region}:${Account}:case/${CaseId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
membership	`arn:${Partition}:security-ir:${Region}:${Account}:membership/${MembershipId}`	aws:ResourceTag/${TagKey}

Chaves de condição para resposta a incidentes de AWS segurança

AWS O Security Incident Response define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Security Lake

O Amazon Security Lake (prefixo de serviço: `securitylake`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Security Lake
- Tipos de recursos definidos pelo Amazon Security Lake
- Chaves de condição do Amazon Security Lake

Ações definidas pelo Amazon Security Lake

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de

condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAwsLogSource	Concede permissão para habilitar qualquer tipo de fonte em qualquer região para contas que façam parte de uma organização confiável ou conta autônoma	Gravar	data-lake *		glue:CreateDatabase glue:CreateTable glue:GetDatabase glue:GetTable iam:CreateServiceLinkedRole kms:CreateGrant

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					kms:DescribeKey

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateCustomLogSource	Concede permissão para adicionar uma origem personalizada	Gravar	data-lake *		glue:CreateCrawler glue:CreateDatabase glue:CreateTable glue:StartCrawlerSchedule iam:DeleteRolePolicy iam:GetRole iam:PassRole iam:PutRolePolicy kms:CreateGrant kms:DescribeKey

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					kms:GenerateDataKey lakeformation:GrantPermissions lakeformation:RegisterResource s3:ListBucket s3:PutObject

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDataLake	Concede permissão para criar um novo data lake de segurança	Gravar	data-lake *		events:PutRule events:PutTargets iam:CreateServiceLinkedRole iam:DeleteRolePolicy iam:GetRole iam:ListAttachedRolePolicies iam:PassRole iam:PutRolePolicy kms:CreateGrant kms:DescribeKey lakeformation:GetD

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ataLakeSettings lakeformation:PutDataLakeSettings lambda:AddPermission lambda:CreateEventSourceMapping lambda:CreateFunction organizations:DescribeOrganization organizations:ListAccounts organizations:ListDelegatedServicesF

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					orAccount s3:CreateBucket s3:GetObject s3:GetObjectVersion s3:ListBucket s3:PutBucketPolicy s3:PutBucketPublicAccessBlock s3:PutBucketVersioning sqs:CreateQueue sqs:GetQueueAttributes

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					sqs:SetQueueAttributes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataLakeExceptionSubscription	Concede permissão para receber notificações instantâneas sobre exceções. Assina os tópicos do SNS para notificações de exceções	Gravar			
CreateDataLakeOrganizationConfiguration	Concede permissão para habilitar automaticamente o Amazon Security Lake para novas contas de membro em sua organização	Gravar	data-lake*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSubscriber	Concede permissão para criar um assinante	Gravar		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	iam:CreateRole iam:DeleteRolePolicy iam:GetRole iam:PutRolePolicy lakeformation:GrantPermissions lakeformation:ListPermissions lakeformation:RegisterResource lakeformation:RevokePermissions

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					ram:GetResourceShareAssociations ram:GetResourceShares ram:UpdateResourceShare s3:PutObject

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSubscriberNotification	Concede permissão para criar uma invocação de webhook para notificar um cliente quando há novos dados no data lake	Gravar	subscriber*		events:CreateApiDestination events:CreateConnection events:DescribeRule events:ListApiDestinations events:ListConnections events:PutRule events:PutTargets iam:DeleteRolePolicy iam:GetRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					iam:PassRole s3:GetBucketNotification s3:PutBucketNotification sqs:CreateQueue sqs:DeleteQueue sqs:GetQueueAttributes sqs:GetQueueUrl sqs:SetQueueAttributes
DeleteAwsLogSource	Concede permissão para desabilitar qualquer tipo de fonte em qualquer região para contas que fazem parte de uma organização confiável ou contas independentes	Gravar	data-lake*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteCustomLogSource	Concede permissão para remover uma fonte personalizada	Gravar	data-lake*		glue:StopCrawlerSchedule
DeleteDataLake	Concede permissão para excluir data lake de segurança	Gravar	data-lake*		organizations:DescribeOrganization organizations:ListDelegatedAdministrators organizations:ListDelegatedServicesForAccount
DeleteDataLakeExceptionSubscription	Concede permissão para cancelar a assinatura de tópicos do SNS para notificações de exceções. Remove notificações de exceção para o tópico SNS	Gravar			
DeleteDataLakeOrganizationConfiguration	Concede permissão para remover a ativação automática do acesso do Amazon Security Lake para novas contas da organização	Gravar	data-lake*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteSubscriber	Concede permissão para excluir o assinante especificado	Gravar	subscriber*		events:DeleteApiDestination events:DeleteConnection events:DeleteRule events:DescribeRule events:ListApiDestinations events:ListTargetsByRule events:RemoveTargets iam:DeleteRole iam:DeleteRolePolicy

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					iam:GetRole iam:ListRolePolicies lakeformation:ListPermissions lakeformation:RevokePermissions sqs:DeleteQueue sqs:GetQueueUrl

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteSubscriberNotification	Concede permissão para remover uma invocação de webhook para notificar um cliente quando há novos dados no data lake	Gravar	subscriber*		events:DeleteApiDestination events:DeleteConnection events:DeleteRule events:DescribeRule events:ListApiDestinations events:ListTargetsByRule events:RemoveTargets iam:DeleteRole iam:DeleteRolePolicy

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					iam:GetRole iam:ListRolePolicies lakeformation:RevokePermissions sqs:DeleteQueue sqs:GetQueueUrl
DeregisterDataLakeDelegatedAdministrator	Concede permissão para remover a conta de administrador delegado e desabilitar o Amazon Security Lake como um serviço para essa organização	Gravar			organizations:DeregisterDelegatedAdministrator organizations:DescribeOrganization organizations:ListDelegatedServicesForAccount

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetDataLakeExceptionSubscription	Concede permissão para consultar o protocolo e o endpoint que foram fornecidos ao se inscrever em tópicos do SNS para notificações de exceção	Leitura			
GetDataLakeOrganizationConfiguration	Concede permissão para obter a definição de configuração de uma organização para habilitar automaticamente o acesso do Amazon Security Lake para novas contas da organização	Leitura	data-lake*		organizations:DescribeOrganization
GetDataLakeSources	Concede permissão para obter um instantâneo estático do data lake de segurança na região atual. O instantâneo inclui contas habilitadas e origens de log	Leitura	data-lake*		
GetSubscriber	Concede permissão para obter informações sobre um assinante que já foi criado	Leitura	subscriber*		
ListDataLakeExceptions	Concede permissão para obter a lista de todas as falhas que não podem ser repetidas	Lista			
ListDataLakes	Concede permissão para listar informações sobre os data lakes de segurança	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListLogSources	Concede permissão para visualizar as contas habilitadas. Você pode ver as fontes habilitadas nas regiões habilitadas	Lista			
ListSubscribers	Concede permissão para listar todos os assinantes	Lista			
ListTagsForResource	Concede permissão para listar todas as tags do recurso	Lista	data-lake		
			subscriber		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RegisterDataLakeDelegatedAdministrator	Concede permissão para designar uma conta como a conta de administrador do Amazon Security Lake para a organização	Gravar			iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators organizations:ListDelegatedServicesForAccount organizations:RegisterDelegatedAdministrator

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para adicionar tags ao recurso	Tags	data-lake		
			subscriber		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover tags do recurso	Tags	data-lake		
			subscriber		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateDataLake	Concede permissão para atualizar um data lake de segurança	Gravar	data-lake*		events:PutRule events:PutTargets iam:CreateServiceLinkedRole iam:DeleteRolePolicy iam:GetRole iam:ListAttachedRolePolicies iam:PutRolePolicy kms:CreateGrant kms:DescribeKey lakeformation:GetDataLakeSettings

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					lakeformation:PutDataLakeSettings lambda:AddPermission lambda:CreateEventSourceMapping lambda:CreateFunction organizations:DescribeOrganization organizations:ListDelegatedServicesForAccount s3:CreateBucket s3:GetObject

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					s3:GetObjectVersion s3:ListBucket s3:PutBucketPolicy s3:PutBucketPublicAccessBlock s3:PutBucketVersioning sqs:CreateQueue sqs:GetQueueAttributes sqs:SetQueueAttributes
UpdateDataLakeExceptionSubscription	Concede permissão para atualizar assinaturas nos tópicos do SNS para notificações de exceções	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateSubscriber	Concede permissão para atualizar um assinante	Gravar	subscriber*		events:CreateApiDestination events:CreateConnection events:DescribeRule events:ListApiDestinations events:ListConnections events:PutRule events:PutTargets iam:DeleteRolePolicy iam:GetRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					iam:PutRolePolicy

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateSubscriberNotification	Concede permissão para atualizar uma invocação de webhook para notificar um cliente quando há novos dados no data lake	Gravar	subscriber*		events:CreateApiDestination events:CreateConnection events:DescribeRule events:ListApiDestinations events:ListConnections events:PutRule events:PutTargets iam:CreateServiceLinkedRole iam:DeleteRolePolicy

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					iam:GetRole iam:PassRole iam:PutRolePolicy s3:CreateBucket s3:GetBucketNotification s3:ListBucket s3:PutBucketNotification s3:PutBucketPolicy s3:PutBucketPublicAccessBlock s3:PutBucketVersioning

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					s3:PutLifecycleConfiguration sqs:CreateQueue sqs:DeleteQueue sqs:GetQueueAttributes sqs:GetQueueUrl sqs:SetQueueAttributes

Tipos de recursos definidos pelo Amazon Security Lake

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do Amazon Security Lake

O Amazon Security Lake define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por um par de chave e valor da etiqueta de um recurso.	String
aws:TagKeys	Filtra o acesso pelas chaves de etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Server Migration Service

AWS O Server Migration Service (prefixo do serviço:`sms`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Server Migration Service
- Tipos de recursos definidos pelo AWS Server Migration Service
- Chaves de condição do AWS Server Migration Service

Ações definidas pelo AWS Server Migration Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateApp	Concede permissão para criar uma configuração de aplicativo para migrar o aplicativo local para AWS	Gravar			
CreateReplicationJob	Concede permissão para criar um trabalho para migrar o servidor local para AWS	Gravar			
DeleteApp	Concede permissão para excluir uma configuração de aplicativo existente	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteAppLaunchConfiguration	Concede permissão para excluir a configuração de execução de um aplicativo existente	Write			
DeleteAppReplicationConfiguration	Concede permissão para excluir a configuração de replicação de um aplicativo existente	Write			
DeleteAppValidationConfiguration	Concede permissão para excluir a configuração de validação de um aplicativo existente	Gravar			
DeleteReplicationJob	Concede permissão para excluir um trabalho existente para migrar o servidor local para AWS	Gravar			
DeleteServerCatalog	Concede permissão para excluir a lista completa de servidores locais reunidos em AWS	Gravar			
DisassociateConnector	Concede permissão para desassociar um conector que foi associado	Gravar			
GenerateChangeSet	Concede permissão para gerar um ChangeSet para a pilha de um CloudFormation aplicativo	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GenerateTemplate	Concede permissão para gerar um CloudFormation modelo para um aplicativo existente	Gravar			
GetApp	Concede permissão para obter a configuração e os status de um aplicativo existente	Read			
GetAppLaunchConfiguration	Concede permissão para obter a configuração de execução de um aplicativo existente	Read			
GetAppReplicationConfiguration	Concede permissão para obter a configuração de replicação de um aplicativo existente	Read			
GetAppValidationConfiguration	Concede permissão para obter configuração de validação de um aplicativo existente	Read			
GetAppValidationOutput	Concede permissão para obter notificação enviada do script de validação do aplicativo.	Read			
GetConnectors	Concede permissão para obter todos os conectores que foram associados	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetMessages [somente permissão]	Concede permissão para receber mensagens do AWS Server Migration Service para o Server Migration Connector	Leitura			
GetReplicationJobs	Concede permissão para que todos os trabalhos existentes migrem servidores locais para AWS	Leitura			
GetReplicationRuns	Concede permissão para obter todas as execuções de um trabalho existente	Read			
GetServers	Concede permissão para obter todos os servidores que foram importados	Leitura			
ImportAppCatalog	Concede permissão para importar o catálogo de aplicativos do AWS Application Discovery Service	Gravar			
ImportServerCatalog	Concede permissão para reunir uma lista completa de servidores locais	Gravar			
LaunchApp	Concede permissão para criar e iniciar uma CloudFormation pilha para um aplicativo existente	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListApps	Concede permissão para obter uma lista de resumos para aplicativos existentes	List			
NotifyAppValidationOutput	Concede permissão para enviar notificações para o script de validação do aplicativo	Write			
PutAppLaunchConfiguration	Concede permissão para criar ou atualizar a configuração de execução de um aplicativo existente	Write			
PutAppReplicationConfiguration	Concede permissão para criar ou atualizar a configuração de replicação de um aplicativo existente	Write			
PutAppValidationConfiguration	Concede permissão para colocar a configuração de validação de um aplicativo existente	Write			
SendMessage [somente permissão]	Concede permissão para enviar mensagem do Conector de Migração do Servidor para o Serviço de Migração AWS do Servidor	Gravar			
StartAppReplication	Concede permissão para criar e iniciar trabalhos de replicação para um aplicativo existente	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartOnDemandAppReplication	Concede permissão para iniciar uma execução de replicação para um aplicativo existente	Write			
StartOnDemandReplicationRun	Concede permissão para iniciar uma execução de replicação para um trabalho de replicação existente	Write			
StopAppReplication	Concede permissão para interromper e excluir trabalhos de replicação de um aplicativo existente	Gravar			
TerminateApp	Concede permissão para encerrar a CloudFormation pilha de um aplicativo existente	Gravar			
UpdateApp	Concede permissão para atualizar a configuração de um aplicativo existente	Gravar			
UpdateReplicationJob	Concede permissão para atualizar um trabalho existente para migrar o servidor local para AWS	Gravar			

Tipos de recursos definidos pelo AWS Server Migration Service

AWS O Server Migration Service não oferece suporte à especificação de um ARN de recurso `Resource` no elemento de uma declaração de política do IAM. Para conceder acesso ao AWS Server Migration Service, especifique `"Resource": "*"` na política.

Chaves de condição do AWS Server Migration Service

ServerMigrationService não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Serverless Application Repository

AWS O Serverless Application Repository (prefixo do serviço`serverlessrepo`:) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Serverless Application Repository
- Tipos de recursos definidos pelo AWS Serverless Application Repository
- Chaves de condição do AWS Serverless Application Repository

Ações definidas pelo AWS Serverless Application Repository

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou

ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateApplication	Concede permissão para criar um aplicativo, incluindo opcionalmente um arquivo AWS SAM para criar a primeira versão do aplicativo na mesma chamada	Gravar			
CreateApplicationVersion	Concede permissão para criar uma versão da aplicação	Gravar	applications*		
CreateCloudFormationChangeSet	Concede permissão para criar um AWS CloudFormation ChangeSet para o aplicativo em questão	Gravar	applications*		
				serverlessrepo:applicationType	
CreateCloudFormationTemplate	Concede permissão para criar um AWS CloudFormation modelo	Gravar	applications*		
				serverlessrepo:applicationType	
DeleteApplication	Concede permissão para excluir a aplicação especificada	Gravar	applications*		
GetApplication	Concede permissão para obter a aplicação especificada	Leitura	applications*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				serverlessrepo:applicationType	
GetApplicationPolicy	Concede permissão para obter a política para a aplicação especificada	Leitura	applications*		
GetCloudFormationTemplate	Concede permissão para obter o AWS CloudFormation modelo especificado	Leitura	applications*		
ListApplicationDependencies	Concede permissão para recuperar as aplicações aninhadas na aplicação que as contém	Lista	applications*		
				serverlessrepo:applicationType	
ListApplicationVersions	Concede permissão para listar versões da aplicação especificada pertencentes ao solicitante	Lista	applications*		
				serverlessrepo:applicationType	
ListApplications	Concede permissão para listar as aplicações que pertencem ao solicitante	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutApplicationPolicy	Concede permissão para introduzir a política na aplicação especificada	Gravar	applications*		
SearchApplications	Concede permissão para obter todas as aplicações autorizadas para este usuário	Leitura		serverlessrepo:applicationType	
UnshareApplication	Concede permissão para descompartilhar a aplicação especificada	Gravar	applications*		
UpdateApplication	Concede permissão para atualizar os metadados de uma aplicação	Gravar	applications*		

Tipos de recursos definidos pelo AWS Serverless Application Repository

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
applications	`arn:${Partition}:serverlessrepo:${Region}:${Account}:applications/${ResourceId}`	

Chaves de condição do AWS Serverless Application Repository

AWS O Serverless Application Repository define as seguintes chaves de condição que podem ser usadas no elemento de uma política `Condition` do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
serverlessrepo:applicationType	Filtra o acesso por tipo de aplicação	String

Ações, recursos e chaves de condição para AWS Service - Oracle Database@AWS

AWS Serviço - O Oracle Database@AWS (prefixo do serviço:odb) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Serviço - Oracle Database@AWS
- Tipos de recursos definidos pelo AWS Serviço - Oracle Database@AWS
- Chaves de condição para AWS Service - Oracle Database@AWS

Ações definidas pelo AWS Serviço - Oracle Database@AWS

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptMarketplaceRegistration	Concede permissão para registrar o token do Amazon Web Services Marketplace para sua conta da Amazon Web Services para ativar sua assinatura do Oracle Database @Amazon Web Services	Gravar			
CreateCloudAutonomousVmCluster	Concede permissão para criar um novo cluster de VM autônoma na infraestrutura especificada do Exadata	Gravar	cloud-exadata-infrastructure*		
			odb-network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudExadataInfrastructure	Concede permissão para criar uma infraestrutura do Exadata	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateCloudVmCluster	Concede permissão para criar um cluster de VM na infraestrutura especificada do Exadata	Gravar	cloud-exadata-infrastructure*		
			odb-network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDbNode [somente permissão]	Concede permissão para criar um nó de banco de dados	Gravar	db-node*		
CreateOdbNetwork	Concede permissão para criar uma rede ODB	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOdbPeeringConnection	Concede permissão para criar uma conexão de emparelhamento ODB	Gravar	odb-network*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateOutboundIntegration [somente permissão]	Concede permissão para criar uma integração externa	Gravar	cloud-autonomous-vm-cluster*		
			cloud-vm-cluster*		
DeleteCloudAutonomousVmCluster	Concede permissão para excluir um cluster de VM autônoma	Gravar	cloud-autonomous-vm-cluster*		
DeleteCloudExadataInfrastructure	Concede permissão para excluir uma infraestrutura específica do Exadata. Antes de usar essa operação, certifique-se de excluir todos os clusters de VM hospedados nessa infraestrutura do Exadata.	Gravar	cloud-exadata-infrastructure*		
DeleteCloudVmCluster	Concede permissão para excluir um cluster de VM especificado	Gravar	cloud-vm-cluster*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteDbNode [somente permissão]	Concede permissão para excluir um nó de banco de dados	Gravar	db-node*		
DeleteOdbNetwork	Concede permissão para excluir a rede ODB especificada	Gravar	odb-network*		
DeleteOdbPeeringConnection	Concede permissão para excluir a conexão de emparelhamento ODB especificada. Quando você exclui uma conexão de emparelhamento ODB, a conexão de emparelhamento de VPC subjacente também é excluída	Gravar	odb-peering-connection*		
DeleteResourcePolicy [somente permissão]	Concede permissão para excluir uma política de recurso	Gravar	cloud-exadata-infrastructure*		
			odb-network*		
GetCloudAutonomousVmCluster	Concede permissão para obter informações sobre um cluster de VM autônoma específico	Leitura	cloud-autonomous-vm-cluster*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetCloudExadataInfrastructure	Concede permissão para obter informações sobre a infraestrutura especificada do Exadata	Leitura	cloud-exadata-infrastructure*		
GetCloudExadataInfrastructureUnallocatedResources	Concede permissão para recuperar informações sobre recursos não alocados em uma infraestrutura específica do Cloud Exadata	Leitura	cloud-exadata-infrastructure*		
GetCloudVmCluster	Concede permissão para obter informações sobre o cluster de VM especificado	Leitura	cloud-vm-cluster*		
GetDbNode	Concede permissão para obter informações sobre o nó de banco de dados especificado	Leitura	cloud-vm-cluster*		
			db-node*		
GetDbServer	Concede permissão para obter informações sobre o servidor de banco de dados especificado	Leitura	cloud-exadata-infrastructure*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetOciOnboardingStatus	Concede permissão para obter o link de ativação da locação e o status de integração da sua conta da Amazon Web Services	Leitura			
GetOdbNetwork	Concede permissão para obter informações sobre a rede ODB especificada	Leitura	odb-network*		
GetOdbPeeringConnection	Concede permissão para obter informações sobre a conexão de emparelhamento ODB especificada	Leitura	odb-peering-connection*		
GetResourcePolicy [somente permissão]	Concede permissão para obter uma política de recurso	Leitura	cloud-exadata-infrastructure*		
			odb-network*		
InitializeService	Concede permissão para inicializar o serviço ODB pela primeira vez em uma conta	Gravar			
ListAutonomousVirtualMachines	Concede permissão para listar todos os Autonomous VMs em um cluster de VM autônomo	Leitura	cloud-autonomous-vm-cluster		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListCloudAutonomousVmClusters	Concede permissão para listar todos os clusters de VMs autônomas em uma infraestrutura específica do Cloud Exadata	Lista	cloud-exadata-infrastructure		
ListCloudExadataInfrastructures	Concede permissão para listar informações sobre as infraestruturas do Exadata pertencentes à sua conta da Amazon Web Services	Lista			
ListCloudVmClusters	Concede permissão para listar informações sobre os clusters de VM pertencentes à sua conta da Amazon Web Services ou somente aqueles na infraestrutura especificada do Exadata	Lista	cloud-exadata-infrastructure		
ListDbNodes	Concede permissão para listar informações sobre os nós de banco de dados para o cluster de VM especificado	Lista	cloud-vm-cluster*		
ListDbServers	Concede permissão para listar informações sobre os servidores de banco de dados que pertencem à infraestrutura especificada do Exadata	Leitura	cloud-exadata-infrastructure*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDbSystemShapes	Concede permissão para listar informações sobre as formas que estão disponíveis para uma infraestrutura do Exadata	Leitura			
ListGiVersions	Concede permissão para listar informações sobre as versões do software Oracle Grid Infrastructure (GI) que estão disponíveis para um cluster de VM na forma especificada	Leitura			
ListOdbNetworks	Concede permissão para listar informações sobre as redes ODB pertencentes à sua conta da Amazon Web Services	Lista			
ListOdbPeeringConnections	Concede permissão para listar todas as conexões de emparelhamento ODB ou aquelas associadas a uma rede ODB específica	Lista	odb-network		
ListSystemVersions	Concede permissão para listar informações sobre as versões do sistema que estão disponíveis para um cluster de VM para a giVersion e a forma especificadas	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar informações sobre as tags aplicadas a esse recurso	Leitura	cloud-autonomous-vm-cluster		
			cloud-exadata-infrastructure		
			cloud-vm-cluster		
			db-node		
			odb-network		
			odb-peering-connection		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutResourcePolicy [somente permissão]	Concede permissão para atualizar uma política de recurso	Gravar	cloud-exadata-infrastructure*		
			odb-network*		
RebootDbNode	Concede permissão para reinicializar o nó de banco de dados especificado em um cluster de VM	Gravar	cloud-vm-cluster*		
			db-node*		
StartDbNode	Concede permissão para iniciar o nó de banco de dados especificado em um cluster de VM	Gravar	cloud-vm-cluster*		
			db-node*		
StopDbNode	Concede permissão para interromper o nó de banco de dados especificado em um cluster de VM	Gravar	cloud-vm-cluster*		
TagResource	Concede permissão para aplicar tags ao recurso especificado	Tags	cloud-autonomous-vm-cluster		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			cloud-exadata-infrastructure		
			cloud-vm-cluster		
			db-node		
			odb-network		
			odb-peering-connection		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para remover tags do recurso especificado	Tags	cloud-autonomous-vm-cluster		
			cloud-exadata-infrastructure		
			cloud-vm-cluster		
			db-node		
			odb-network		
			odb-peering-connection		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateCloudExadataInfrastructure	Concede permissão para atualizar as propriedades de um recurso de infraestrutura do Exadata	Gravar	cloud-exadata-infrastructure*		
UpdateOdbNetwork	Concede permissão para atualizar as propriedades de uma rede ODB especificada	Gravar	odb-network*		

Tipos de recursos definidos pelo AWS Serviço - Oracle Database@AWS

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
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}

Chaves de condição para AWS Service - Oracle Database@AWS

AWS Serviço - O Oracle Database@AWS define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por um par de chave valor da etiqueta que é permitido na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso por um par de chave e valor da etiqueta de um recurso.	Segmento

Chaves de condição	Descrição	Tipo
aws:TagKeys	Filtra o acesso por uma lista de chaves da etiqueta que são permitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Service Catalog

AWS O Service Catalog (prefixo do serviço:`servicecatalog`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Service Catalog
- Tipos de recursos definidos pelo AWS Service Catalog
- Chaves de condição do AWS Service Catalog

Ações definidas pelo AWS Service Catalog

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptPortfolioShare	Concede permissão para aceitar um portfólio que foi compartilhado com você	Write	Portfolio*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateAttributeGroup	Concede permissão para associar um grupo de atributos a uma aplicação	Write	Application*		
			AttributeGroup*		
AssociateBudgetWithResource	Concede permissão para associar um orçamento a um recurso	Write			
AssociatePrincipalWithPortfolio	Concede permissão para associar um principal do IAM a um portfólio, concedendo ao principal especificado acesso a todos os produtos associados ao portfólio especificado	Write	Portfolio*		
AssociateProductWithPortfolio	Concede permissão para associar um produto a um portfólio	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateResource	Concede permissão para associar um recurso a uma aplicação	Write	Application*		cloudformation:DescribeStacks resource-groups:CreateGroup resource-groups:GetGroup resource-groups:Tag
				servicecatalog:ResourceType servicecatalog:Resource	
AssociateServiceActionWithProvisioningArtifact	Concede permissão para associar uma ação a um artefato de provisionamento	Gravar	Product*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateTagOptionWithResource	Concede permissão para associar o especificado TagOption ao portfólio ou produto especificado	Gravar	Portfolio		
			Product		
BatchAssociateServiceActionWithProvisioningArtifact	Concede permissão para associar várias ações de autoatendimento a artefatos de provisionamento	Write			
BatchDisassociateServiceActionFromProvisioningArtifact	Concede permissão para desassociar um lote de ações de autoatendimento do artefato de provisionamento especificado	Write			
CopyProduct	Concede permissão para copiar o produto de origem especificado no produto de destino especificado ou em um novo produto	Write			
CreateApplication	Concede permissão para criar um aplicativo	Write	Application*		iam:CreateServiceLinkedRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAttributeGroup	Concede permissão para criar um grupo de atributos	Write	AttributeGroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConstraint	Concede permissão para criar uma restrição em um produto e um portfólio associados	Write	Product*		
CreatePortfolio	Concede permissão para criar um portfólio	Gravar	Portfolio*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePortfolioShare	Concede permissão para compartilhar um portfólio que você possui com outra pessoa Conta da AWS	Gerenciamento de permissões	Portfolio*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateProduct	Concede permissão para criar um produto e o primeiro artefato de provisionamento desse produto	Write	Product*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProvisionedProductPlan	Concede permissão para adicionar um novo plano de produto provisionado	Write		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
CreateProvisioningArtifact	Concede permissão para adicionar um novo artefato de provisionamento a um produto existente	Write	Product*		
CreateServiceAction	Concede permissão para criar uma ação de autoatendimento	Gravar			
CreateTagOption	Concede permissão para criar um TagOption	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteApplication	Concede permissão para excluir uma aplicação se todas as associações tiverem sido removidas da aplicação	Write	Application*		
DeleteAttributeGroup	Concede permissão para excluir um grupo de atributos se todas as associações tiverem sido removidas do grupo de atributos	Write	AttributeGroup*		
DeleteConstraint	Concede permissão para remover e excluir uma restrição existente de um produto e um portfólio associados	Write			
DeletePortfolio	Concede permissão para excluir um portfólio se todas as associações e os compartilhamentos tiverem sido removidos do portfólio	Gravar	Portfolio*		
DeletePortfolioShare	Concede permissão para cancelar o compartilhamento de um portfólio que você possui e com o Conta da AWS qual você compartilhou o portfólio anteriormente	Gerenciamento de permissões	Portfolio*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteProduct	Concede permissão para excluir um produto se todas as associações tiverem sido removidas do produto	Write	Product*		
DeleteProvisionedProductPlan	Concede permissão para excluir um plano de produto provisionado	Write		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DeleteProvisioningArtifact	Concede permissão para excluir um artefato de provisionamento de um produto	Gravar	Product*		
DeleteResourcePolicy [somente permissão]	Concede permissão para excluir uma política baseada em recursos para o recurso especificado	Gravar	Application		
			AttributeGroup		
DeleteServiceAction	Concede permissão para excluir uma ação de autoatendimento	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteTagOption	Concede permissão para excluir o especificado TagOption	Gravar			
DescribeConstraint	Concede permissão para descrever uma restrição	Read			
DescribeCopyProductStatus	Concede permissão para obter o status da operação de cópia especificada do produto	Read			
DescribePortfolio	Concede permissão para descrever um portfólio	Read	Portfolio*		
DescribePortfolioShareStatus	Concede permissão para obter o status da operação de compartilhamento de portfólio especificada	Read			
DescribePortfolioShares	Concede permissão para exibir um resumo de cada um dos compartilhamentos do portfólio que foram criados para o portfólio especificado	List	Portfolio*		
DescribeProduct	Concede permissão para descrever um produto como um usuário final	Read	Product*		
DescribeProductAsAdmin	Concede permissão para descrever um produto como administrador	Read	Product*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeProductView	Concede permissão para descrever um produto como um usuário final	Read			
DescribeProvisionedProduct	Concede permissão para descrever um produto provisionado	Read		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DescribeProvisionedProductPlan	Concede permissão para descrever um plano de produto provisionado	Read		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DescribeProvisioningArtifact	Concede permissão para descrever um artefato de provisionamento	Read	Product*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeProvisioningParameters	Concede permissão para descrever os parâmetros que você precisa especificar para provisionar um artefato de provisionamento especificado com êxito	Read	Product*		
DescribeRecord	Concede permissão para descrever um registro e lista todas as saídas	Read		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DescribeServiceAction	Concede permissão para descrever uma ação de autoatendimento	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeServiceActionExecutionParameters	Concede permissão para obter os parâmetros padrão se você executou a ação de serviço especificada no produto provisionado especificado	Leitura		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DescribeTagOption	Concede permissão para obter informações sobre o especificado TagOption	Leitura			
DisableAWSOrganizationsAccess	Concede permissão para desativar o compartilhamento de portfólio por meio do recurso AWS Organizations	Gravar			
DisassociateAttributeGroup	Concede permissão para desassociar um grupo de atributos de uma aplicação	Write	Application* AttributeGroup*		
DisassociateBudgetFromResource	Concede permissão para desassociar um orçamento de um recurso	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociatePrincipalFromPortfolio	Concede permissão para desassociar um principal do IAM de um portfólio	Write	Portfolio*		
DisassociateProductFromPortfolio	Concede permissão para desassociar um produto de um portfólio	Write			
DisassociateResource	Concede permissão para desassociar um recurso de uma aplicação	Write	Application*		resource-groups:DeleteGroup
				servicecatalog:ResourceType servicecatalog:Resource	
DisassociateServiceActionFromProvisioningArtifact	Concede permissão para desassociar a associação da ação de autoatendimento especificada do artefato de provisionamento especificado	Gravar	Product*		
DisassociateTagOptionFromResource	Concede permissão para desassociar o recurso especificado TagOption do especificado	Gravar	Portfolio		
			Product		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
EnableAWSOrganizationsAccess	Concede permissão para ativar o recurso de compartilhamento de portfólio por meio de AWS Organizations	Gravar			
ExecuteProvisionedProductPlan	Concede permissão para executar um plano de produto provisionado	Write		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ExecuteProvisionedProductServiceAction	Concede permissão para executar um plano de produto provisionado	Gravar		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAWSOrganizationsAccessStatus	Concede permissão para obter o status de acesso do recurso de compartilhamento do portfólio da AWS organização	Leitura			
GetApplication	Concede permissão para obter uma aplicação	Read	Application*		
GetAssociatedResource	Concede permissão para obter informações sobre um recurso associado a uma aplicação	Read	Application*		
				servicecatalog:ResourceType servicecatalog:Resource	
GetAttributeGroup	Concede permissão para obter um grupo de atributos	Leitura	AttributeGroup*		
GetConfiguration	Concede permissão para ler as AppRegistry configurações	Leitura			
GetProvisionedProductOutputs	Concede permissão para obter a saída do produto provisionado com o ID ou nome do produto provisionado	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetResourcePolicy [somente permissão]	Concede permissão para obter uma política baseada em recursos para o recurso especificado	Leitura	Application		
			AttributeGroup		
ImportAsProvisionedProduct	Concede permissão para importar um recurso para um produto provisionado	Write	Product*		
ListAcceptedPortfolioShares	Concede permissão para listar os portfólios que foram compartilhados com você e foram aceitos	Lista			
ListApplications	Concede permissão para listar suas aplicações	Lista			
ListAssociatedAttributeGroups	Concede permissão para listar os grupos de atributos associados a uma aplicação	List	Application*		
ListAssociatedResources	Concede permissão para listar os recursos associados a uma aplicação	Lista	Application*		
ListAttributeGroups	Concede permissão para listar seus grupos de atributos	Lista			
ListAttributeGroupsForApplication	Concede permissão para listar os grupos de atributos associados a uma determinada aplicação	Lista	Application*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListBudgetsForResource	Concede permissão para listar todos os orçamentos associados a um recurso	List			
ListConstraintsForPortfolio	Concede permissão para listar as restrições associadas a determinado portfólio	List			
ListLaunchPaths	Concede permissão para listar as diferentes maneiras de lançar determinado produto como um usuário final	List	Product*		
ListOrganizationPortfolioAccess	Concede permissão para listar os nós da organização que têm acesso ao portfólio especificado	Lista			
ListPortfolioAccess	Concede permissão para listar as AWS contas com as quais você compartilhou um determinado portfólio	Lista	Portfolio*		
ListPortfolios	Concede permissão para listar os portfólios na conta	List			
ListPortfoliosForProduct	Concede permissão para listar os portfólios associados a determinado produto	List	Product*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListPrincipalsForPortfolio	Concede permissão para listar os principais do IAM associados a determinado portfólio	List	Portfolio*		
ListProvisionedProductPlans	Concede permissão para listar os planos de produtos provisionados	List		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ListProvisioningArtifacts	Concede permissão para listar os artefatos de provisionamento associados a determinado produto	List	Product*		
ListProvisioningArtifactsForServiceAction	Concede permissão para listar todos os artefatos de provisionamento para a ação de autoatendimento especificada	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListRecordHistory	Concede permissão para listar todos os registros na conta ou todos os registros relacionados a determinado produto provisionado	Lista		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ListResourcesForTagOption	Concede permissão para listar os recursos associados ao especificado TagOption	Lista			
ListServiceActions	Concede permissão para listar todas as ações de autoatendimento	List			
ListServiceActionsForProvisioningArtifact	Concede permissão para listar todas as ações de serviço associadas ao artefato de provisionamento especificado na conta	List	Product*		
				servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListStackInstancesForProvisionedProduct	Concede permissão para listar a conta, a região e o status de cada instância de pilha associada a um produto provisionado do tipo CFN_STACKSET	Lista		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ListTagOptions	Concede permissão para listar o especificado TagOptions ou todos TagOptions	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso do AppRegistry do catálogo de serviços	Leitura	Application		
			AttributeGroup		
NotifyProvisionProductEngineWorkflowResult	Concede permissão para notificar o resultado da execução do mecanismo de provisionamento	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
NotifyTerminateProvisionedProductEngineWorkflowResult	Concede permissão para notificar o resultado da execução do mecanismo de término	Gravar			
NotifyUpdateProvisionedProductEngineWorkflowResult	Concede permissão para notificar o resultado da execução do mecanismo de atualização	Gravar			
ProvisionProduct	Concede permissão para provisionar um produto com um artefato de provisionamento e parâmetros de execução especificados	Gravar	Product*		
PutConfiguration	Concede permissão para atribuir AppRegistry configurações	Gravar			
PutResourcePolicy [somente permissão]	Concede permissão para adicionar uma política baseada em recursos para o recurso especificado	Gravar	Application		
			AttributeGroup		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RejectPortfolioShare	Concede permissão para rejeitar um portfólio que foi compartilhado com você e que foi aceito anteriormente	Write	Portfolio*		
ScanProvisionedProducts	Concede permissão para listar todos os produtos provisionados na conta	List		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
SearchProducts	Concede permissão para listar os produtos disponíveis para você como usuário final	List			
SearchProductsAsAdmin	Concede permissão para listar todos os produtos na conta ou todos os produtos associados a determinado portfólio	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SearchProvisionedProducts	Concede permissão para listar todos os produtos provisionados na conta	Lista		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
SyncResource	Concede permissão para sincronizar um recurso com seu estado atual no AppRegistry	Gravar			cloudformation:UpdateStack
TagResource	Concede permissão para marcar um recurso do AppRegistry do catálogo de serviços	Marcação	Application		
			AttributeGroup		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TerminateProvisionedProduct	Concede permissão para encerrar um produto provisionado existente	Write		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
UntagResource	Concede permissão para remover uma etiqueta de um recurso do AppRegistry do catálogo de serviços	Marcação	Application		
			AttributeGroup		
				aws:TagKeys	
UpdateApplication	Concede permissão para atualizar os atributos de uma aplicação existente	Write	Application*		iam:CreateServiceLinkedRole
UpdateAttributeGroup	Concede permissão para atualizar os atributos de um grupo de atributos existente	Write	AttributeGroup*		
UpdateConstraint	Concede permissão para atualizar os campos de metadados de uma restrição existente	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdatePortfolio	Concede permissão para atualizar as and/or tags dos campos de metadados de um portfólio existente	Gravar	Portfolio*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdatePortfolioShare	Concede permissão para ativar ou desativar o compartilhamento de recursos para um compartilhamento de portfólio existente	Gerenciamento de permissões	Portfolio*		
UpdateProduct	Concede permissão para atualizar as and/or tags dos campos de metadados de um produto existente	Gravar	Product*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateProvisionedProduct	Concede permissão para atualizar um produto provisionado existente	Write		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
UpdateProvisionedProductProperties	Concede permissão para atualizar as propriedades de um produto provisionado existente	Write			
UpdateProvisioningArtifact	Concede permissão para atualizar os campos de metadados de um artefato de provisionamento existente	Write	Product*		
UpdateServiceAction	Concede permissão para atualizar uma ação de autoatendimento	Gravar			
UpdateTagOption	Concede permissão para atualizar o especificado TagOption	Gravar			

Tipos de recursos definidos pelo AWS Service Catalog

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS Service Catalog

AWS O Service Catalog define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

> **Note**
>
> Para obter exemplos de políticas que mostram como estas chaves de condição podem ser usadas em uma política do IAM, consulte Exemplo de políticas de acesso para gerenciamento de produtos provisionados no Guia do administrador do catálogo de serviços.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString
servicecatalog:Resource	Filtra o acesso controlando qual valor pode ser especificado como o parâmetro Resource em uma API de recursos AppRegistry associada	String
servicecatalog:ResourceType	Filtra o acesso controlando qual valor pode ser especificado como ResourceType parâmetro em uma API de recursos AppRegistry associada	String
servicecatalog:accountLevel	Filtra o acesso pelo usuário que pode ver e executar ações em recursos criados por qualquer pessoa na conta	String
servicecatalog:roleLevel	Filtra o acesso pelo usuário que pode ver e executar ações em recursos criados por eles ou por qualquer pessoa federada na mesma função que eles	String
servicecatalog:userLevel	Filtra o acesso pelo usuário que podem ver e executar ações apenas em recursos que criaram	String

Ações, recursos e chaves de condição do AWS Serviço para gerenciar recursos de experiência AWS Management Console do usuário.

AWS Serviço para gerenciar recursos AWS Management Console de experiência do usuário. (prefixo do serviço:`uxc`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Serviço para gerenciar os recursos de experiência AWS Management Console do usuário.
- Tipos de recursos definidos pelo AWS Serviço para gerenciar os recursos de experiência AWS Management Console do usuário.
- Chaves de condição do AWS Serviço para gerenciar recursos de experiência AWS Management Console do usuário.

Ações definidas pelo AWS Serviço para gerenciar os recursos de experiência AWS Management Console do usuário.

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteAccountColor	Concede permissão para excluir a cor associada à conta	Gravar			
GetAccountColor	Concede permissão para obter a cor associada à conta	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutAccountColor	Concede permissão para definir a cor associada a uma conta	Gravar			

Tipos de recursos definidos pelo AWS Serviço para gerenciar os recursos de experiência AWS Management Console do usuário.

AWS O serviço para gerenciar recursos de experiência AWS Management Console do usuário não oferece suporte à especificação de um ARN de recurso no elemento de uma declaração de política `Resource` do IAM. Para permitir o acesso ao AWS Serviço para gerenciar os recursos de experiência AWS Management Console do usuário, especifique `"Resource": "*"` em sua política.

Chaves de condição do AWS Serviço para gerenciar recursos de experiência AWS Management Console do usuário.

A Personalização da Experiência do Usuário (UXC) não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o serviço da AWS que fornece redes privadas gerenciadas

AWS O serviço que fornece redes privadas gerenciadas (prefixo do serviço:`private-networks`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo serviço da AWS que fornece redes privadas gerenciadas
- Tipos de recursos definidos pelo serviço da AWS que fornece redes privadas gerenciadas
- Chaves de condição para o serviço da AWS que fornece redes privadas gerenciadas

Ações definidas pelo serviço da AWS que fornece redes privadas gerenciadas

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcknowledgeOrderReceipt	Concede permissão para confirmar que um pedido foi recebido	Gravar	order*		
ActivateDeviceIdentifier	Concede permissão para ativar um identificador de dispositivo	Gravar	device-identifier*		
				aws:ResourceTag/${TagKey}	
ActivateNetworkSite	Concede permissão para ativar uma instalação de rede		network-site*		
			order*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ConfigureAccessPoint	Concede permissão para configurar um ponto de acesso	Gravar	network-resource*		
CreateNetwork	Concede permissão para criar uma rede	Gravar	network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNetworkSite	Concede permissão para criar uma instalação de rede	Gravar	network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeactivateDeviceIdentifier	Concede permissão para desativar um identificador de dispositivo	Gravar	device-identifier*		
DeleteNetwork	Concede permissão para excluir uma rede	Gravar	network*		
DeleteNetworkSite	Concede permissão para excluir uma instalação de rede	Gravar	network-site*		
GetDeviceIdentifier	Concede permissão para obter um identificador de dispositivo	Leitura	device-identifier*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
GetNetwork	Concede permissão para obter uma rede	Leitura	network*		
				aws:ResourceTag/${TagKey}	
GetNetworkResource	Concede permissão para obter um recurso de rede	Leitura	network-resource*		
				aws:ResourceTag/${TagKey}	
GetNetworkSite	Concede permissão para obter uma instalação de rede	Leitura	network-site*		
				aws:ResourceTag/${TagKey}	
GetOrder	Concede permissão para obter um pedido de rede	Leitura	order*		
				aws:ResourceTag/${TagKey}	
ListDeviceIdentifiers	Concede permissão para listar identificadores de dispositivo	Lista	network*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListNetworkResources	Concede permissão para listar recursos de rede	Lista	network*		
ListNetworkSites	Concede permissão para listar instalações de rede	Lista	network*		
ListNetworks	Concede permissão para listar redes	Lista			
ListOrders	Concede permissão para listar pedidos de rede	Lista	network*		
ListTagsForResource	Concede permissão para retornar uma lista de etiquetas de um recurso	Lista			
Ping	Concede permissão para verificar a integridade do serviço	Leitura			
StartNetworkResourceUpdate	Concede permissão para iniciar uma atualização no recurso de rede especificado	Gravar	network-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Concede permissão para adicionar etiquetas ao recurso especificado	Tags	device-identifier		
			network		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			network-resource		
			network-site		
			order		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover etiquetas do recurso especificado.	Tags	device-identifier		
			network		
			network-resource		
			network-site		
			order		
				aws:TagKeys	
UpdateNetworkSite	Concede permissão para atualizar uma instalação de rede	Gravar	network-site*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateNetworkSitePlan	Concede permissão para atualizar um plano em uma instalação de rede	Gravar	network-site*		

Tipos de recursos definidos pelo serviço da AWS que fornece redes privadas gerenciadas

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Tipos de recursos	ARN	Chaves de condição
device-identifier	`arn:${Partition}:private-networks:${Region}:${Account}:device-identifier/${NetworkName}/${DeviceId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o serviço da AWS que fornece redes privadas gerenciadas

AWS O serviço que fornece redes privadas gerenciadas define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso verificando a presença de pares de chave-valor de etiquetas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso verificando pares de chave-valor de etiquetas anexadas ao recurso	String
aws:TagKeys	Filtra acesso pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Service Quotas

O Service Quotas (prefixo do serviço: `servicequotas`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Service Quotas
- Tipos de recursos definidos pelo Service Quotas
- Chaves de condição do Service Quotas

Ações definidas pelo Service Quotas

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de

condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateServiceQuotaTemplate	Concede permissão para associar o modelo do Service Quotas à sua organização	Gravar			organizations:DescribeOrganization organizations:EnableAWSServiceAccess
CreateSupportCase	Concede permissão para enviar uma solicitação para criar um caso de suporte para uma solicitação existente de aumento de cota	Gravar			
DeleteServiceQuotaIncreaseR	Concede permissão para remover a cota de serviço	Write			organizations:Desc

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
equestFromTemplate	especificada do modelo de cota de serviço				ribeOrganization
DisassociateServiceQuotaTemplate	Concede permissão para desassociar o modelo do Service Quotas de sua organização	Gravar			organizations:DescribeOrganization
GetAWSDefaultServiceQuota	Concede permissão para retornar os detalhes da cota de serviço especificada, incluindo o AWS valor padrão	Leitura			
GetAssociationForServiceQuotaTemplate	Concede permissão para recuperar o ServiceQuotaTemplateAssociationStatus valor, que informa se o modelo de Quotas de Serviço está associado a uma organização	Leitura			organizations:DescribeOrganization
GetRequestedServiceQuotaChange	Concede permissão para recuperar os detalhes de uma determinada solicitação de aumento de cota de serviço	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetServiceQuota	Concede permissão para retornar os detalhes da cota de serviço especificada, incluindo o valor aplicado	Read			autoscaling:DescribeAccountLimits cloudformation:DescribeAccountLimits dynamodb:DescribeLimits elasticloadbalancing:DescribeAccountLimits iam:GetAccountSummary kinesis:DescribeLimits rds:DescribeAccountAttributes

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					route53:GetAccountLimit
GetServiceQuotaIncreaseRequestFromTemplate	Concede permissão para recuperar os detalhes de uma solicitação de aumento de cota de serviço do modelo de cota de serviço	Leitura			organizations:DescribeOrganization
ListAWSDefaultServiceQuotas	Concede permissão para listar todas as cotas de serviço padrão para o serviço especificado AWS	Leitura			
ListRequestedServiceQuotaChangeHistory	Concede permissão para solicitar uma lista de alterações em cotas de um serviço	Read			
ListRequestedServiceQuotaChangeHistoryByQuota	Concede permissão para solicitar uma lista de alterações em cotas de serviço específicas	Read			
ListServiceQuotaIncreaseRequestsInTemplate	Concede permissão para retornar uma lista de solicitações de aumento de cota de serviço do modelo de cota de serviço	Leitura			organizations:DescribeOrganization

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListServiceQuotas	Concede permissão para listar todas as cotas de serviço para o AWS serviço especificado, nessa conta, nessa região	Leitura			autoscaling:DescribeAccountLimits cloudformation:DescribeAccountLimits dynamodb:DescribeLimits elasticloadbalancing:DescribeAccountLimits iam:GetAccountSummary kinesis:DescribeLimits rds:DescribeAccountAttributes

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					route53:GetAccountLimit
ListServices	Concede permissão para listar os AWS serviços disponíveis em Service Quotas	Leitura			
ListTagsForResource	Concede permissão para exibir as etiquetas existentes em um recurso SQ	Leitura			
PutServiceQuotaIncreaseRequestIntoTemplate	Concede permissão para definir e adicionar uma cota ao modelo de cota de serviço	Write	quota		organizations:DescribeOrganization
				servicequotas:service	
RequestServiceQuotaIncrease	Concede permissão para enviar a solicitação para um aumento de cota de serviço	Write	quota		
				servicequotas:service	
TagResource	Concede permissão para associar um conjunto de etiquetas a um recurso SQ existente	Marcação		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para remover um conjunto da etiquetas de um recurso SQ, onde as etiquetas a serem removidas correspondem a um conjunto de chaves da etiqueta fornecidas pelo cliente	Marcação		aws:TagKeys	

Tipos de recursos definidos pelo Service Quotas

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
quota	`arn:${Partition}:servicequotas:${Region}:${Account}:${ServiceCode}/${QuotaCode}`	

Chaves de condição do Service Quotas

O Service Quotas define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString
servicequotas:service	Filtra o acesso pelo AWS serviço especificado	String

Ações, recursos e chaves de condição do Amazon SES

O Amazon SES (prefixo do serviço: `ses`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon SES
- Tipos de recursos definidos pelo Amazon SES
- Chaves de condição do Amazon SES

Ações definidas pelo Amazon SES

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CloneReceiptRuleSet	Concede permissão para criar um conjunto de regras de recebimento clonando uma existente	Write		ses:ApiVersion	
CreateConfigurationSet	Concede permissão para criar um novo conjunto de configurações	Write		ses:ApiVersion	
CreateConfigurationSetEventDestination	Concede permissão para criar um destino de evento do conjunto de configuração	Write		ses:ApiVersion	
CreateConfigurationSetTrackingOptions	Concede permissão para criar uma associação entre um conjunto de configurações e um domínio personalizado para rastreamento de eventos de abertura e de clique	Write		ses:ApiVersion	
CreateCustomVerificationEmailTemplate	Concede permissão para criar um novo modelo de e-mail de verificação personalizado	Write		ses:ApiVersion	
CreateReceiptFilter	Concede permissão para criar um novo filtro de endereço IP	Write		ses:ApiVersion	
CreateReceiptRule	Concede permissão para criar uma regra de recebimento	Write		ses:ApiVersion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateReceiptRuleSet	Concede permissão para criar um conjunto de regras de recebimento vazio	Write		ses:ApiVersion	
CreateTemplate	Concede permissão para criar um modelo de e-mail	Write		ses:ApiVersion	
DeleteConfigurationSet	Concede permissão para excluir um conjunto de configurações existente	Write		ses:ApiVersion	
DeleteConfigurationSetEventDestination	Concede permissão para excluir um destino de evento	Write		ses:ApiVersion	
DeleteConfigurationSetTrackingOptions	Concede permissão para excluir uma associação entre um conjunto de configurações e um domínio personalizado para rastreamento de eventos de abertura e de clique	Write		ses:ApiVersion	
DeleteCustomVerificationEmailTemplate	Concede permissão para excluir um modelo de e-mail de verificação personalizado existente	Write		ses:ApiVersion	
DeleteIdentity	Concede permissão para excluir a identidade especificada	Write		ses:ApiVersion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteIdentityPolicy	Concede permissão para excluir a política de autorização de envio especificada para a determinada identidade (um endereço de e-mail ou um domínio)	Permissions management		ses:ApiVersion	
DeleteReceiptFilter	Concede permissão para excluir o filtro de endereço IP especificado	Write		ses:ApiVersion	
DeleteReceiptRule	Concede permissão para excluir a regra de recebimento especificado	Write		ses:ApiVersion	
DeleteReceiptRuleSet	Concede permissão para excluir o conjunto de regras de recebimento especificado e todas as regras de recebimento que ele contém	Write		ses:ApiVersion	
DeleteTemplate	Concede permissão para excluir um modelo de e-mail	Write		ses:ApiVersion	
DeleteVerifiedEmailAddress	Concede permissão para excluir o endereço de e-mail especificado da lista de endereços verificados	Write		ses:ApiVersion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeActiveReceiptRuleSet	Concede permissão para retornar os metadados e as regras de recebimento do conjunto de regras de recebimento que está ativo no momento	Read		ses:ApiVersion	
DescribeConfigurationSet	Concede permissão para retornar os detalhes do conjunto de configurações especificado	Read		ses:ApiVersion	
DescribeReceiptRule	Concede permissão para retornar os detalhes da regra de recebimento especificada	Read		ses:ApiVersion	
DescribeReceiptRuleSet	Concede permissão para retornar os detalhes do conjunto de regras de recebimento especificado	Read		ses:ApiVersion	
GetAccountSendingEnabled	Concede permissão para devolver o status de envio de e-mail da sua conta	Read		ses:ApiVersion	
GetCustomVerificationEmailTemplate	Concede permissão para retornar o modelo de verificação de e-mail personalizado para o nome do modelo especificado	Read		ses:ApiVersion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetIdentityDkimAttributes	Concede permissão para retornar o status atual da assinatura Easy DKIM para uma entidade	Leitura		ses:ApiVersion	
GetIdentityMailFromDomainAttributes	Concede permissão para retornar os atributos MAIL FROM personalizados para uma lista de identidades (and/or domínios de endereços de e-mail)	Leitura		ses:ApiVersion	
GetIdentityNotificationAttributes	Concede permissão para retornar uma estrutura descrevendo os atributos de notificação de identidade para uma lista de identidades verificadas (and/or domínios de endereços de e-mail),	Leitura		ses:ApiVersion	
GetIdentityPolicies	Concede permissão para retornar as políticas de autorização de envio solicitadas para a determinada identidade (um endereço de e-mail ou um domínio)	Read		ses:ApiVersion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetIdentityVerificationAttributes	Concede permissão para retornar o status de verificação e (para identidades de domínio) o token de verificação para uma lista de identidades	Read		ses:ApiVersion	
GetSendQuota	Concede permissão para retornar os limites do envio atuais do usuário	Read		ses:ApiVersion	
GetSendStatistics	Concede permissão para retornar as estatísticas de envio do usuário	Read		ses:ApiVersion	
GetTemplate	Concede permissão para retornar o objeto do modelo, que inclui a linha de assunto, parte HTML e parte de texto do modelo que você especificar	Read		ses:ApiVersion	
ListConfigurationSets	Concede permissão para listar todos os conjuntos de configuração da sua conta	List		ses:ApiVersion	
ListCustomVerificationEmailTemplates	Concede permissão para listar todos os modelos de e-mail de verificação personalizados existentes para sua conta	List		ses:ApiVersion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListIdentities	Concede permissão para listar as identidades de e-mail da sua conta	List		ses:ApiVersion	
ListIdentityPolicies	Concede permissão para listar todos os modelos de e-mail da sua conta	List		ses:ApiVersion	
ListReceiptFilters	Concede permissão para listar os filtros de endereço IP associados à sua conta	Read		ses:ApiVersion	
ListReceiptRuleSets	Concede permissão para listar os conjuntos de regras de recebimento que existem na sua conta	Read		ses:ApiVersion	
ListTemplates	Concede permissão para listar os modelos de e-mail presentes na sua conta	List		ses:ApiVersion	
ListVerifiedEmailAddresses	Concede permissão para listar todos os endereços de e-mail que foram verificados em sua conta	Read		ses:ApiVersion	
PutConfigurationSetDeliveryOptions	Concede permissão para adicionar ou atualizar as opções de entrega de um conjunto de configurações	Write		ses:ApiVersion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutIdentityPolicy	Concede permissão para adicionar ou atualizar a política de autorização de envio para determinada identidade (um endereço de e-mail ou um domínio)	Permissions management		ses:ApiVersion	
ReorderReceiptRuleSet	Concede permissão para reordenar as regras de recebimento dentro de um conjunto de regras de recebimento	Write		ses:ApiVersion	
SendBounce	Concede permissão para gerar e enviar uma mensagem de devolução ao remetente de um e-mail recebido por meio do Amazon SES	Write	identity*		
				ses:ApiVersion ses:FromAddress	
SendBulkTemplatedEmail	Concede permissão para compor uma mensagem de e-mail para vários destinos	Write	identity*		
			template*		
			configuration-set		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SendCustomVerificationEmail	Concede permissão para adicionar um endereço de e-mail à lista de identidades e tenta verificá-lo para sua conta	Write	identity*		
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SendEmail	Concede permissão para enviar uma mensagem de e-mail	Write	identity*		
			configuration-set		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SendRawEmail	Concede permissão para enviar uma mensagem de e-mail, com cabeçalho e conteúdo especificados pelo cliente	Write	identity* configuration-set		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SendTemplatedEmail	Concede permissão para compor uma mensagem de e-mail usando um modelo de e-mail	Write	identity*		
			template*		
			configuration-set		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SetActiveReceiptRuleSet	Concede permissão para definir o conjunto de regras de recebimento especificado como o conjunto de regras de recebimento ativo	Write		ses:ApiVersion	
SetIdentityDkimEnabled	Concede permissão para habilitar ou desabilitar a assinatura Easy DKIM de e-mail enviado a partir de uma identidade	Write		ses:ApiVersion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SetIdentityFeedbackForwardingEnabled	Concede permissão para habilitar ou desabilitar se o Amazon SES encaminha notificações de devolução e reclamação para uma identidade (um endereço de e-mail ou um domínio)	Write		ses:ApiVersion	
SetIdentityHeadersInNotificationsEnabled	Concede permissão para definir se o Amazon SES inclui os cabeçalhos de e-mail originais nas notificações do Amazon Simple Notification Service (Amazon SNS) de um tipo especificado para determinada identidade (um endereço de e-mail ou um domínio)	Write		ses:ApiVersion	
SetIdentityMailFromDomain	Concede permissão para habilitar ou desabilitar a configuração de domínio MAIL FROM personalizada para uma identidade verificada	Write		ses:ApiVersion	
SetIdentityNotificationTopic	Concede permissão para definir um tópico do Amazon Simple Notification Service (Amazon SNS) a ser usado ao entregar notificações para uma identidade verificada	Write		ses:ApiVersion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SetReceiptRulePosition	Concede permissão para definir a posição da regra de recebimento especificada no conjunto de regras de recebimento	Write		ses:ApiVersion	
TestRenderTemplate	Concede permissão para criar uma visualização do conteúdo MIME de um e-mail quando fornecido com um modelo e um conjunto de dados de substituição	Write		ses:ApiVersion	
UpdateAccountSendingEnabled	Concede permissão para habilitar ou desabilitar o envio de e-mail para sua conta	Write		ses:ApiVersion	
UpdateConfigurationSetEventDestination	Concede permissão para atualizar o destino do evento de um conjunto de configurações	Write		ses:ApiVersion	
UpdateConfigurationSetReputationMetricsEnabled	Concede permissão para habilitar ou desabilitar a publicação de métricas de reputação para e-mails enviados usando um conjunto de configuração específico	Write		ses:ApiVersion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateConfigurationSetSendingEnabled	Concede permissão para habilitar ou desabilitar o envio de e-mails para mensagens enviadas usando um conjunto de configurações específico	Write		ses:ApiVersion	
UpdateConfigurationSetTrackingOptions	Concede permissão para modificar uma associação entre um conjunto de configurações e um domínio personalizado para rastreamento de eventos abertos e cliques	Write		ses:ApiVersion	
UpdateCustomVerificationEmailTemplate	Concede permissão para atualizar um modelo de e-mail de verificação personalizado existente	Write		ses:ApiVersion	
UpdateReceiptRule	Concede permissão para atualizar uma regra de recebimento	Write		ses:ApiVersion	
UpdateTemplate	Concede permissão para atualizar um modelo de e-mail	Write		ses:ApiVersion	
VerifyDomainDkim	Concede permissão para retornar um conjunto de tokens DKIM de um domínio	Gravar		ses:ApiVersion	
VerifyDomainIdentity	Concede permissão para verificar um domínio	Gravar		ses:ApiVersion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
VerifyEmailAddress	Concede permissão para verificar um endereço de e-mail	Gravar		ses:ApiVersion	
VerifyEmailIdentity	Concede permissão para verificar uma identidade de e-mail	Gravar		ses:ApiVersion	

Tipos de recursos definidos pelo Amazon SES

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
template	`arn:${Partition}:ses:${Region}:${Account}:template/${TemplateName}`	

Chaves de condição do Amazon SES

O Amazon SES define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
ses:ApiVersion	Filtra as ações com base na versão da API SES	String
ses:FeedbackAddress	Filtra ações com base no endereço "Return-Path" que especifica para onde as devoluções e reclamações são enviadas por encaminhamento de comentários por e-mail.	String
ses:FromAddress	Filtra ações com base no endereço “De” de uma mensagem	String
ses:FromDisplayName	Filtra ações com base no endereço “De” que é usado como o nome de exibição de uma mensagem	String
ses:Recipients	Filtra ações com base nos endereços de destinatários de uma mensagem que incluem os endereços "Para", "CC" e "BCC".	ArrayOfString

Ações, recursos e chaves de condição do AWS Shield

AWS O Shield (prefixo do serviço:`shield`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Shield
- Tipos de recursos definidos pelo AWS Shield
- Chaves de condição do AWS Shield

Ações definidas pelo AWS Shield

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateDRTLogBucket	Concede permissão para autorizar a equipe do DDo S Response a acessar o bucket do Amazon S3 especificado contendo seus registros de fluxo	Gravar			s3:GetBucketPolicy s3:PutBucketPolicy
AssociateDRTRole	Concede permissão para autorizar a equipe do DDo S Response, usando a função especificada, a acessar sua Conta da AWS para ajudar na	Gravar			iam:GetRole iam:ListAttachedRolePolicies

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	mitigação do ataque DDo S durante possíveis ataques				iam:PassRole
Associate HealthCheck	Concede permissão para adicionar detecção baseada em saúde à proteção do Shield Advanced para um recurso	Gravar	protection*		route53:GetHealthCheck
				aws:ResourceTag/${TagKey}	
Associate Proactive EngagementDetails	Concede permissão para inicializar o engajamento proativo e definir a lista de contatos para o DDo S Response Team (DRT) usar	Gravar			
CreateProtection	Concede permissão para ativar o serviço de proteção DDo S para um determinado ARN de recurso	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProtectionGroup	Concede permissão para criar um agrupamento de recursos protegidos para que eles possam ser tratados como um coletivo	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscription	Concede permissão para ativar a assinatura	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteProtection	Concede permissão para excluir uma proteção existente	Write	protection*		
				aws:ResourceTag/${TagKey}	
DeleteProtectionGroup	Concede permissão para remover o grupo de proteção especificado	Write	protection-group*		
				aws:ResourceTag/${TagKey}	
DeleteSubscription	Concede permissão para desativar a assinatura	Write			
DescribeAttack	Concede permissão para obter detalhes de ataque	Leitura	attack*		
DescribeAttackContributors [somente permissão]	Concede permissão para obter informações detalhadas sobre os contribuidores de um ataque DDo S específico	Leitura	attack*		
			protection-group		
DescribeAttackStatistics	Concede permissão para descrever informações sobre o número e o tipo de ataques que a AWS Shield detectou no último ano	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeDRTAccess	Concede permissão para descrever a função atual e a lista de buckets de log do Amazon S3 usados pela equipe do DDo S Response para acessá-los Conta da AWS enquanto auxilia na mitigação de ataques	Leitura			
DescribeEmergencyContactSettings	Concede permissão para listar os endereços de e-mail que o DRT pode usar para entrar em contato com você durante um ataque suspeito	Read			
DescribeProtection	Concede permissão para obter detalhes de proteção	Read	protection*		
				aws:ResourceTag/${TagKey}	
DescribeProtectionGroup	Concede permissão para descrever a especificação para o grupo de proteção especificado	Read	protection-group*		
				aws:ResourceTag/${TagKey}	
DescribeSubscription	Concede permissão para obter detalhes da assinatura, como hora de início	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisableApplicationLayerAutomaticResponse	Concede permissão para desabilitar a resposta automática da camada da aplicação para proteção do Shield Advanced de um recurso	Gravar			
DisableProactiveEngagement	Concede permissão para remover a autorização da Equipe de Resposta DDoS (DRT) para notificar os contatos sobre escalonamentos	Gravar			
DisassociateDRTLogBucket	Concede permissão para remover o acesso da equipe do DDoS Response ao bucket especificado do Amazon S3 contendo seus registros de fluxo	Gravar			s3:DeleteBucketPolicy s3:GetBucketPolicy s3:PutBucketPolicy
DisassociateDRTRole	Concede permissão para remover o acesso da equipe do DDoS Response ao seu Conta da AWS	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateHealthCheck	Concede permissão para remover a detecção baseada em integridade da proteção do Shield Advanced para um recurso	Gravar	protection*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
EnableApplicationLayerAutomaticResponse	Concede permissão para habilitar a resposta automática da camada da aplicação para proteção do Shield Advanced de um recurso	Gravar			apprunner:DescribeWebAclForService cloudfront:GetDistribution cognito-idp:GetWebACLForResource ec2:GetVerifiedAccessInstanceWebAcl iam:CreateServiceLinkedRole iam:GetRole wafv2:GetWebACL wafv2:GetWebACLForResource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
EnableProactiveEngagement	Concede permissão para autorizar a Equipe de Resposta DDo S (DRT) a usar e-mail e telefone para notificar os contatos sobre escalonamentos	Gravar			
GetGlobalThreatData [somente permissão]	Concede permissão para recuperar dados e tendências globais de inteligência de ameaças dos sistemas de monitoramento de ameaças da AWS Shield	Leitura			
GetSubscriptionState	Concede permissão para obter o estado da assinatura	Read			
ListAttacks	Concede permissão para listar todos os ataques existentes	Lista			
ListMitigations [somente permissão]	Concede permissão para recuperar uma lista de ações de mitigação que foram aplicadas durante os ataques S DDo	Lista	attack*		
ListProtectionGroups	Concede permissão para recuperar os grupos de proteção da conta	List			
ListProtections	Concede permissão para listar todas as proteções existentes	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListResourcesInProtectionGroup	Concede permissão para recuperar os recursos incluídos no grupo de proteção	Lista	protection-group*		
ListTagsForResource	Concede permissão para obter informações sobre AWS tags para um Amazon Resource Name (ARN) especificado no Shield AWS	Leitura	protection		
			protection-group		
TagResource	Concede permissão para adicionar ou atualizar tags para um recurso no AWS Shield	Tags	protection		
			protection-group		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover tags de um recurso no AWS Shield	Tags	protection		
			protection-group		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateApplicationLayerAutomaticResponse	Concede permissão para atualizar a resposta automática da camada da aplicação para proteção do Shield Advanced de um recurso	Gravar			apprunner:DescribeWebAclForService cognito-idp:GetWebACLForResource ec2:GetVerifiedAccessInstanceWebAcl wafv2:GetWebACL wafv2:GetWebACLForResource
UpdateEmergencyContactSettings	Concede permissão para atualizar os detalhes da lista de endereços de e-mail que o DRT pode usar para entrar em contato com você durante um ataque suspeito	Write			
UpdateProtectionGroup	Concede permissão para atualizar um grupo de proteção existente	Write	protection-group*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
UpdateSubscription	Concede permissão para atualizar os detalhes de uma assinatura existente	Write			

Tipos de recursos definidos pelo AWS Shield

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS Shield

AWS O Shield define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base na presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra ações com base nos pares de chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações com base na presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o diretor de segurança de rede AWS Shield

AWS O diretor de segurança de rede Shield (prefixo de serviço:`network-security-director`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo diretor de segurança de rede da AWS Shield
- Tipos de recursos definidos pelo diretor de segurança de rede AWS Shield
- Chaves de condição para o diretor de segurança de rede AWS Shield

Ações definidas pelo diretor de segurança de rede da AWS Shield

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de

recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetFinding	Concede permissão para obter uma descoberta	Leitura			
GetNetworkSecurityScan	Concede permissão para obter o status da verificação de segurança da rede	Leitura			
GetResource	Concede permissão para obter um recurso	Leitura			
ListFindings	Concede permissão para listar as descobertas	Lista			
ListInsights	Concede permissão para listar informações sobre a verificação de segurança de rede mais recente	Lista			
ListRemediations	Concede permissão para listar as remediações para uma descoberta	Lista			
ListResources	Concede permissão para listar recursos	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartNetworkSecurityScan	Concede permissão para iniciar uma verificação de segurança de rede	Gravar			
UpdateFinding	Concede permissão para atualizar o status de uma descoberta	Gravar			

Tipos de recursos definidos pelo diretor de segurança de rede AWS Shield

AWS O diretor de segurança de rede Shield não suporta a especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para permitir o acesso ao diretor de segurança de rede AWS Shield, especifique `"Resource": "*"` em sua política.

Chaves de condição para o diretor de segurança de rede AWS Shield

O Network Security Director não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o AWS Signer

AWS Signer (prefixo do serviço:`signer`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Signer
- Tipos de recursos definidos pelo AWS Signer
- Chaves de condição do AWS Signer

Ações definidas pelo AWS Signer

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de

recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddProfilePermission	Concede permissão para adicionar permissões entre contas a um perfil de assinatura	Permissions management	signing-profile*		
CancelSigningProfile	Concede permissão para alterar o estado de um perfil de assinatura para CANCELADO	Write	signing-profile*		
				signer:ProfileVersion	
DescribeSigningJob	Concede permissão para retornar informações sobre um trabalho de assinatura específico	Leitura	signing-job*		
GetRevocationStatus	Concede permissão para consultar informações de revogação de recursos de assinatura	Leitura	signing-job*		
			signing-profile*		
GetSigningPlatform	Concede permissão para devolver informações sobre	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	uma plataforma de assinatura específica				
GetSigningProfile	Concede permissão para retornar informações sobre um perfil de assinatura específico	Read	signing-profile*		
				signer:ProfileVersion	
ListProfilePermissions	Concede permissão para listar as permissões entre contas associadas a um perfil de assinatura	Read	signing-profile*		
ListSigningJobs	Concede permissão para listar todos os trabalhos de assinatura em sua conta	List			
ListSigningPlatforms	Concede permissão para listar todas as plataformas de assinatura disponíveis	List			
ListSigningProfiles	Concede permissão para listar todos os perfis de assinatura em sua conta	List			
ListTagsForResource	Concede permissão para listar as etiquetas associadas a um perfil de assinatura	Read	signing-profile*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutSigningProfile	Concede permissão para criar um novo perfil de assinatura	Write		aws:RequestTag/${TagKey} aws:TagKeys	
RemoveProfilePermission	Concede permissão para remover permissões entre contas de um perfil de assinatura	Permissions management	signing-profile*		
RevokeSignature	Concede permissão para alterar o estado de um trabalho de assinatura para REVOGADO	Write	signing-job*		
				signer:ProfileVersion	
RevokeSigningProfile	Concede permissão para alterar o estado de um perfil de assinatura para REVOGADO	Gravar	signing-profile*		
				signer:ProfileVersion	
SignPayload	Concede permissão para iniciar uma trabalho de assinatura na payload fornecida	Gravar	signing-profile*		
				signer:ProfileVersion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartSigningJob	Concede permissão para iniciar uma trabalho de assinatura no código fornecido	Write	signing-profile*		
				signer:ProfileVersion	
TagResource	Concede permissão para adicionar uma ou mais etiquetas a um perfil de assinatura	Marcação	signing-profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover uma ou mais etiquetas de um perfil de assinatura	Marcação	signing-profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Tipos de recursos definidos pelo AWS Signer

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves

são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
signing-profile	`arn:${Partition}:signer:${Region}:${Account}:/signing-profiles/${ProfileName}`	aws:ResourceTag/${TagKey}
signing-job	`arn:${Partition}:signer:${Region}:${Account}:/signing-jobs/${JobId}`	

Chaves de condição do AWS Signer

AWS O signatário define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por conjunto de valores permitido para cada uma das etiquetas	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelo valor-etiqueta associado ao recurso	String
aws:TagKeys	Filtra o acesso por presença de etiquetas obrigatórias na solicitação	ArrayOfString
signer:ProfileVersion	Filtra o acesso por versão do perfil de assinatura	String

Ações, recursos e chaves de condição do AWS Signin

AWS O login (prefixo do serviço:`signin`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Signin
- Tipos de recursos definidos pelo AWS Signin
- Chaves de condição do AWS Signin

Ações definidas pelo AWS Signin

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateTrustedIdentityPropagationApplicationForConsole	Concede permissão para criar um aplicativo do Identity Center que represente o AWS Management Console em uma instância da organização do Identity Center	Gravar			sso:CreateApplication sso:GetSharedSsoConfiguration sso:ListApplications

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					sso:PutApplicationAccessScope sso:PutApplicationAssignmentConfiguration sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant
ListTrustedIdentityPropagationApplicationsForConsole	Concede permissão para listar todos os aplicativos do Identity Center que representam o AWS Management Console	Lista			sso:GetSharedSsoConfiguration sso:ListApplications

Tipos de recursos definidos pelo AWS Signin

AWS O login não suporta a especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para conceder acesso ao AWS Signin, especifique `"Resource": "*"` na política.

Chaves de condição do AWS Signin

O Signin não tem chaves de contexto específicas do serviço que podem ser usadas no elemento `Condition` das instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do Amazon Simple Email Service para Mail Manager

O Mail Manager do Amazon Simple Email Service (prefixo do serviço: `ses`) fornece os recursos, ações e chaves de contexto de condição a seguir específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Mail Manager do Amazon Simple Email Service
- Tipos de recursos definidos pelo Mail Manager do Amazon Simple Email Service
- Chaves de condição do Amazon Simple Email Service para Mail Manager

Ações definidas pelo Mail Manager do Amazon Simple Email Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AllowVendedLogDeliveryForResource [somente permissão]	Concede permissão para configurar a entrega de registros vendidos para recursos do Mail Manager	Gerenciamento de permissões	mailmanager-ingress-point		
			mailmanager-rule-set		
CreateAddonInstance	Concede permissão para criar uma instância de complemento	Gravar		aws:RequestTag/${TagKey} aws:TagKeys ses:AddonSubscriptionArn	
CreateAddonSubscription	Concede permissão para criar uma assinatura de complementos	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAddressList	Concede permissão para criar uma lista de endereços	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAddressListImportJob	Concede permissão para criar um trabalho de importação em uma lista de endereços	Gravar	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
CreateArchive	Concede permissão para criar um arquivo	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateIngressPoint	Concede permissão para criar um ponto de entrada	Gravar		aws:RequestTag/${TagKey} aws:TagKeys ses:MailManagerRuleSetArn ses:MailManagerTrafficPolicyArn	ec2:DescribeVpcEndpoints iam:CreateServiceLinkedRole
CreateRelay	Concede permissão para criar uma retransmissão SMTP	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateRuleSet	Concede permissão para criar um conjunto de regras	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTrafficPolicy	Concede permissão para criar uma política de tráfego	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAddonInstance	Concede permissão para excluir uma instância de complemento	Gravar	addon-instance*		
				aws:RequestTag/${TagKey}	
DeleteAddonSubscription	Concede permissão para excluir uma assinatura de complemento	Gravar	addon-subscription*		
				aws:RequestTag/${TagKey}	
DeleteAddressList	Concede permissão para excluir uma lista de endereços	Gravar	mailmanager-address-list*	aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteArchive	Concede permissão para excluir um arquivamento	Gravar	mailmanager-archive*		
				aws:RequestTag/${TagKey}	
DeleteIngressPoint	Concede permissão para excluir um ponto de ingresso	Gravar	mailmanager-ingress-point*		
				aws:RequestTag/${TagKey}	
DeleteRelay	Concede permissão para excluir uma retransmissão SMTP	Gravar	mailmanager-smtp-relay*		
				aws:RequestTag/${TagKey}	
DeleteRuleSet	Concede permissão para excluir um conjunto de regras	Gravar	mailmanager-rule-set*		
				aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteTrafficPolicy	Concede permissão para excluir um ponto de tráfego	Gravar	mailmanager-traffic-policy*		
				aws:RequestTag/${TagKey}	
DeregisterMemberFromAddressList	Concede permissão para remover um membro de uma lista de endereços	Gravar	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
GetAddonInstance	Concede permissão para obter informações sobre uma instância de complemento	Leitura	addon-instance*		
				aws:RequestTag/${TagKey}	
GetAddonSubscription	Concede permissão para obter informações sobre uma assinatura de complemento	Leitura	addon-subscription*		
				aws:RequestTag/${TagKey}	
GetAddressList	Concede permissão para obter informações sobre uma lista de endereços	Leitura	mailmanager-address-list*	aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAddressListImportJob	Concede permissão para obter informações sobre um trabalho de importação em uma lista de endereços	Leitura	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
GetArchive	Concede permissão para obter informações sobre um arquivo	Leitura	mailmanager-archive*		
				aws:RequestTag/${TagKey}	
GetArchiveExport	Concede permissão para obter informações sobre a exportação de um arquivo	Leitura	mailmanager-archive*		
GetArchiveMessage	Concede permissão para recuperar mensagens arquivadas	Leitura	mailmanager-archive*		
GetArchiveMessageContent	Concede permissão para recuperar conteúdo de mensagens arquivadas	Leitura	mailmanager-archive*		
GetArchiveSearch	Concede permissão para obter informações sobre uma pesquisa	Leitura	mailmanager-archive*		
GetArchiveSearchResults	Concede permissão para obter informações sobre resultados de pesquisa	Leitura	mailmanager-archive*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetIngressPoint	Concede permissão para obter informações sobre um ponto de entrada	Leitura	mailmanager-ingress-point*		
				aws:RequestTag/${TagKey}	
GetMemberOfAddressList	Concede permissão para obter informações sobre um membro em uma lista de endereços	Leitura	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
GetRelay	Concede permissão para obter informações sobre uma retransmissão SMTP	Leitura	mailmanager-smtp-relay*		
				aws:RequestTag/${TagKey}	
GetRuleSet	Concede permissão para obter informações sobre um conjunto de regras	Leitura	mailmanager-rule-set*		
				aws:RequestTag/${TagKey}	
GetTrafficPolicy	Concede permissão para obter informações sobre uma política de tráfego	Leitura	mailmanager-traffic-policy*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey}	
ListAddonInstances	Concede permissão para listar todas as instâncias de complementos associadas à sua conta	Lista			
ListAddonSubscriptions	Concede permissão para listar todas as assinaturas de complementos associadas à sua conta	Lista			
ListAddressListImportJobs	Concede permissão para listar todos os trabalhos de importação associados a uma lista de endereços	Lista	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
ListAddressLists	Concede permissão para listar todas as listas de endereços associadas à sua conta	Lista			
ListArchiveExports	Concede permissão para listar todas as exportações de arquivo associadas à sua conta	Lista			
ListArchiveSearches	Concede permissão para listar todas as pesquisas de arquivo associadas à sua conta	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListArchives	Concede permissão para listar todos os arquivos associados à sua conta	Lista			
ListIngressPoints	Concede permissão para listar todos os pontos de entrada associados à sua conta	Lista			
ListMembersOfAddressList	Concede permissão para listar todos os membros associados a uma lista de endereços	Lista	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
ListRelays	Concede permissão para listar todas as retransmissões SMTP associadas à sua conta	Lista			
ListRuleSets	Concede permissão para listar todos os conjuntos de regras associados à sua conta	Lista			
ListTagsForResource	Concede permissão para listar todas as tags associadas ao recurso	Leitura	addon-instance		
			addon-subscription		
			mailmanager-archive		
			mailmanager-ingress-point		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			mailmanager-rule-set		
			mailmanager-smtp-relay		
			mailmanager-traffic-policy		
ListTrafficPolicies	Concede permissão para listar todas as políticas de tráfego associadas à sua conta	Lista			
RegisterMemberToAddressList	Concede permissão para adicionar um membro a uma lista de endereços	Gravar	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
StartAddressListImportJob	Concede permissão para iniciar um trabalho de importação em uma lista de endereços	Gravar	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
StartArchiveExport	Concede permissão para iniciar uma exportação de arquivo	Gravar	mailmanager-archive*		
StartArchiveSearch	Concede permissão para iniciar uma pesquisa de arquivo	Gravar	mailmanager-archive*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StopAddressListImportJob	Concede permissão para interromper um trabalho de importação em andamento em uma lista de endereços	Gravar	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
StopArchiveExport	Concede permissão para interromper a exportação de arquivo	Gravar	mailmanager-archive*		
StopArchiveSearch	Concede permissão para interromper a pesquisa de arquivos	Gravar	mailmanager-archive*		
TagResource	Concede permissão para adicionar uma ou mais etiquetas (chaves e valores) a um recurso especificado	Marcação	addon-instance		
			addon-subscription		
			mailmanager-address-list		
			mailmanager-archive		
			mailmanager-ingress-point		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			mailmanager-rule-set		
			mailmanager-smtp-relay		
			mailmanager-traffic-policy		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover uma ou mais etiquetas (chaves e valores) de um recurso especificado	Tags	addon-instance		
			addon-subscription		
			mailmanager-address-list		
			mailmanager-archive		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			mailmanager-ingress-point		
			mailmanager-rule-set		
			mailmanager-smtp-relay		
			mailmanager-traffic-policy		
				aws:TagKeys	
UpdateArchive	Concede permissão para atualizar um arquivamento	Gravar	mailmanager-archive*		
				aws:RequestTag/${TagKey}	
UpdateIngressPoint	Concede permissão para atualizar um ponto de entrada	Gravar	mailmanager-ingress-point*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} ses:MailManagerTrafficPolicyArn ses:MailManagerRuleSetArn	
UpdateRelay	Concede permissão para atualizar uma retransmissão SMTP	Gravar	mailmanager-smtp-relay*		
				aws:RequestTag/${TagKey}	
UpdateRuleSet	Concede permissão para atualizar um conjunto de regras	Gravar	mailmanager-rule-set*		
				aws:RequestTag/${TagKey}	
UpdateTrafficPolicy	Concede permissão para atualizar uma política de tráfego	Gravar	mailmanager-traffic-policy*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey}	

Tipos de recursos definidos pelo Mail Manager do Amazon Simple Email Service

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
		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}

Chaves de condição do Amazon Simple Email Service para Mail Manager

O Mail Manager do Amazon Simple Email Service define as chaves de condição a seguir que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString
ses:AddonSubscriptionArn	Filtra o acesso pelo ARN da assinatura do complemento do SES	ARN
ses:MailManagerIngressPointType	Filtra o acesso por tipo de ponto de entrada do Mail Manager do SES, por exemplo, OPEN ou AUTH	String
ses:MailManagerRuleSetArn	Filtra o acesso pelo ARN do conjunto de regras do Mail Manager do SES	ARN
ses:MailManagerTrafficPolicyArn	Filtra o acesso pelo ARN da política de tráfego do Mail Manager do SES	ARN

Ações, recursos e chaves de condição do Amazon Simple Email Service v2

O Amazon Simple Email Service v2 (prefixo de serviço: `ses`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Simple Email Service v2
- Tipos de recursos definidos pelo Amazon Simple Email Service v2
- Chaves de condição para o Amazon Simple Email Service v2

Ações definidas pelo Amazon Simple Email Service v2

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de

recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchGetMetricData	Concede permissão para obter dados de métrica sobre sua atividade	Leitura	configuration-set		
			identity		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CancelExportJob	Concede permissão para cancelar um trabalho de exportação	Gravar	export-job*		
				ses:ApiVersion ses:ExportSourceType	
CreateConfigurationSet	Concede permissão para criar um novo conjunto de configurações	Write	configuration-set*		
			dedicated-ip-pool		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			mailmanager-archive		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateConfigurationSetEventDestination	Concede permissão para criar um destino de evento do conjunto de configuração	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CreateContact	Concede permissão para criar um contato	Write	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateContactList	Concede permissão para criar uma lista de contatos	Write	contact-list*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateCustomVerificationEmailTemplate	Concede permissão para criar um novo modelo de e-mail de verificação personalizado	Write	custom-verification-email-template*		
				ses:ApiVersion	
CreateDedicatedIpPool	Concede permissão para criar um novo grupo de endereços IP dedicados	Write	dedicated-ip-pool*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDeliverabilityTestReport	Concede permissão para criar um novo teste de posicionamento de caixa de entrada preditiva	Write	identity*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateEmailIdentity	Concede permissão para iniciar o processo de verificação de uma identidade de e-mail	Write	identity*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateEmailIdentityPolicy	Concede permissão para criar a política de autorização de envio especificada para determinada identidade	Permissions management	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CreateEmailTemplate	Concede permissão para criar um modelo de e-mail	Gravar	template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ses:ApiVersion	
CreateExportJob	Concede permissão para criar um trabalho de exportação	Gravar		ses:ApiVersion ses:ExportSourceType	
CreateImportJob	Concede permissão para criar um trabalho de importação para um destino de dados	Gravar		ses:ApiVersion	
CreateMultiRegionEndpoint	Concede permissão para criar um novo endpoint multirregional	Gravar		ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
CreateTenant	Concede permissão para criar um novo inquilino	Gravar	tenant*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateTenantResourceAssociation	Concede permissão para associar um recurso do SES a um inquilino	Gravar	configuration-set*		
			identity*		
			template*		
			tenant*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
DeleteConfigurationSet	Concede permissão para excluir um conjunto de configurações existente	Write	configuration-set*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteConfigurationSetEventDestination	Concede permissão para excluir um destino de evento	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteContact	Concede permissão para excluir um contato de uma lista de contatos	Write	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteContactList	Concede permissão para excluir uma lista de contatos com todos os seus contatos	Write	contact-list*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteCustomVerificationEmailTemplate	Concede permissão para excluir um modelo de e-mail de verificação personalizado existente	Write	custom-verification-email-template*		
				ses:ApiVersion	
DeleteDedicatedIpPool	Concede permissão para excluir um grupo de IPs dedicados	Write	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteEmailIdentity	Concede permissão para excluir uma identidade de e-mail	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteEmailIdentityPolicy	Concede permissão para excluir a política de autorização de envio especificada para a determinada identidade (um endereço de e-mail ou um domínio)	Permissions management	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteEmailTemplate	Concede permissão para excluir um modelo de e-mail	Gravar	template*		
				ses:ApiVersion	
DeleteMultiRegionEndpoint	Concede permissão para excluir um endpoint multirregional	Gravar	multi-region-endpoint*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteSuppressedDestination	Concede permissão para remover um endereço de e-mail da lista de supressão da sua conta	Gravar		ses:ApiVersion	
DeleteTenant	Concede permissão para excluir um inquilino	Gravar	tenant*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteTenantResourceAssociation	Concede permissão para remover um recurso SES associado de um inquilino	Gravar	configuration-set*		
			identity*		
			template*		
			tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetAccount	Concede permissão para obter informações sobre o status e os recursos de envio de e-mail para sua conta	Read		ses:ApiVersion	
GetBlacklistReports	Concede permissão para recuperar uma lista das listas de negação nas quais seus endereços IP dedicados ou domínios rastreados aparecem	Read		ses:ApiVersion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetConfigurationSet	Concede permissão para obter informações sobre um conjunto de configurações existente	Read	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetConfigurationSetEventDestinations	Concede permissão para recuperar uma lista de destinos de eventos que estão associados a um conjunto de configurações	Read	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetContact	Concede permissão para devolver um contato de uma lista de contatos	Read	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetContactList	Concede permissão para retornar metadados da lista de contatos	Read	contact-list*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ses:ApiVersion	
GetCustomVerificationEmailTemplate	Concede permissão para retornar o modelo de verificação de e-mail personalizado para o nome do modelo especificado	Read	custom-verification-email-template*		
				ses:ApiVersion	
GetDedicatedIp	Concede permissão para obter informações sobre um endereço IP dedicado	Leitura		ses:ApiVersion	
GetDedicatedIpPool	Concede permissão para obter informações sobre um endereço IP dedicado	Leitura	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDedicatedIps	Concede permissão para listar os endereços IP dedicados um grupo de IPs dedicados	Read	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetDeliverabilityDashboardOptions	Concede permissão para obter o status do painel de capacidade de entrega	Read		ses:ApiVersion	
GetDeliverabilityTestReport	Concede permissão para recuperar os resultados de um teste de posicionamento de caixa de entrada preditiva	Read	deliverability-test-report*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDomainDeliverabilityCampaign	Concede permissão para recuperar todos os dados de capacidade de entrega de uma campanha específica	Read		ses:ApiVersion	
GetDomainStatisticsReport	Concede permissão para recuperar o posicionamento da caixa de entrada e as taxas de envolvimento dos domínios usados para enviar e-mail	Read	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetEmailIdentity	Concede permissão para obter informações sobre uma identidade específica	Read	identity*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetEmailIdentityPolicies	Concede permissão para retornar as políticas de autorização de envio solicitadas para a determinada identidade (um endereço de e-mail ou um domínio)	Read	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetEmailTemplate	Concede permissão para retornar o objeto do modelo, que inclui a linha de assunto, parte HTML e parte de texto que você especificar	Leitura	template*		
				ses:ApiVersion	
GetExportJob	Concede permissão para obter informações sobre um trabalho de exportação	Leitura	export-job*		
				ses:ApiVersion ses:ExportSourceType	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetImportJob	Concede permissão para fornecer informações sobre um trabalho de importação	Leitura	import-job*		
				ses:ApiVersion	
GetMessageInsights	Concede permissão para fornecer insights sobre uma mensagem	Leitura		ses:ApiVersion	
GetMultiRegionEndpoint	Concede permissão para obter informações sobre um endpoint multirregional	Leitura	multi-region-endpoint*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetReputationEntity	Concede permissão para recuperar informações sobre o status de uma entidade de reputação	Leitura	tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSuppressedDestination	Concede permissão para recuperar informações sobre um endereço de e-mail específico que está na lista de supressão da sua conta	Leitura		ses:ApiVersion	
GetTenant	Concede permissão para obter informações sobre um inquilino	Leitura	tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListConfigurationSets	Concede permissão para listar todos os conjuntos de configuração da sua conta	List		ses:ApiVersion	
ListContactLists	Concede permissão para listar todas as listas de contatos disponíveis para sua conta	List		ses:ApiVersion	
ListContacts	Concede permissão para listar os contatos presentes em uma lista de contatos específica	List	contact-list*		
				ses:ApiVersion	
ListCustomVerificationEmailTemplates	Concede permissão para listar todos os modelos de e-mail de verificação personalizados existentes para sua conta	List		ses:ApiVersion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDedicatedIpPools	Concede permissão para listar todos os pools de IP dedicados para sua conta	List		ses:ApiVersion	
ListDeliverabilityTestReports	Concede permissão para recuperar a lista dos testes de posicionamento da caixa de entrada preditivos que você executou, independentemente dos status deles, para sua conta	List		ses:ApiVersion	
ListDomainDeliverabilityCampaigns	Concede permissão para listar dados de capacidade de entrega para campanhas que usaram um domínio específico para enviar e-mails durante um intervalo de tempo especificado	Read		ses:ApiVersion	
ListEmailIdentities	Concede permissão para listar as identidades de e-mail da sua conta	List		ses:ApiVersion	
ListEmailTemplates	Concede permissão para listar todos os modelos de e-mail da sua conta	Lista		ses:ApiVersion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListExportJobs	Concede permissão para listar todos os trabalhos de exportação para sua conta	Lista		ses:ApiVersion ses:ExportSourceType	
ListImportJobs	Concede permissão para listar todos os trabalhos de importação para sua conta	Lista		ses:ApiVersion	
ListMultiRegionEndpoints	Concede permissão para listar todos os endpoints multirregionais da sua conta	Lista		ses:ApiVersion	
ListRecommendations	Concede permissão para listar as recomendações para a sua conta	Leitura	identity		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListReputationEntities	Concede permissão para recuperar uma lista de entidades de reputação	Lista	tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListResourceTenants	Concede permissão para listar todos os inquilinos associados a um recurso do SES	Lista	configuration-set*		
			identity*		
			template*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListSuppressedDestinations	Concede permissão para listar endereços de e-mail que estão na lista de supressão da sua conta	Read		ses:ApiVersion	
ListTagsForResource	Concede permissão para recuperar uma lista das etiquetas (chaves e valores) associadas a um recurso específico para sua conta	Leitura	configuration-set		
			contact-list		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			tenant		
				ses:ApiVersion	
ListTenantResources	Concede permissão para listar todos os recursos associados a um inquilino	Lista	tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListTenants	Concede permissão para listar todos os inquilinos da sua conta	Lista		ses:ApiVersion	
PutAccountDedicatedIpWarmupAttributes	Concede permissão para habilitar ou desabilitar o recurso de aquecimento automático para endereços IP dedicados	Write		ses:ApiVersion	
PutAccountDetails	Concede permissão para atualizar os detalhes da sua conta	Write		ses:ApiVersion	
PutAccountSendingAttributes	Concede permissão para ativar ou desativar a capacidade de enviar e-mail para sua conta	Write		ses:ApiVersion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutAccountSuppressionAttributes	Concede permissão para alterar as configurações da lista de supressão no nível da conta	Gravar		ses:ApiVersion	
PutAccountVdmAttributes	Concede permissão para alterar as configurações do VDM para sua conta	Gravar		ses:ApiVersion	
PutConfigurationSetArchivingOptions	Concede permissão para associar um conjunto de configurações a um arquivo do Mail Manager	Gravar	configuration-set*		
			mailmanager-archive		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetDeliveryOptions	Concede permissão para associar um conjunto de configurações a um grupo de IPs dedicados	Write	configuration-set*		
			dedicated-ip-pool		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetReputationOptions	Concede permissão para habilitar ou desabilitar um conjunto de métricas de reputação para e-mails enviados usando um conjunto de configurações específico	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetSendingOptions	Concede permissão para habilitar ou desabilitar o envio de e-mails para mensagens que usam um conjunto de configurações específico	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutConfigurationSetSuppressionOptions	Concede permissão para especificar as preferências da lista de supressão de conta para um determinado conjunto de configurações	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetTrackingOptions	Concede permissão para especificar um domínio personalizado a ser usado para abrir e clicar em elementos de rastreamento no e-mail que você envia para um determinado conjunto de configurações	Gravar	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetVdmOptions	Concede permissão para substituir as configurações do VDM no nível da conta para um determinado conjunto de configurações	Gravar	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpInPool	Concede permissão para mover um endereço IP dedicado para um grupo de IPs dedicados existente	Gravar	dedicated-ip-pool*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpPoolScalingAttributes	Concede permissão para fazer a transição de um pool de IP dedicado de Padrão para Gerenciado	Gravar	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpWarmupAttributes	Concede permissão para colocar atributos de aquecimento de IP dedicado	Write		ses:ApiVersion	
PutDeliverabilityDashboardOption	Concede permissão para habilitar ou desabilitar o painel de capacidade de entrega	Write		ses:ApiVersion	
PutEmailIdentityConfigurationSetAttributes	Concede permissão para associar um conjunto de configurações a uma identidade de e-mail	Write	identity*		
			configuration-set		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityDkimAttributes	Concede permissão para habilitar ou desabilitar a autenticação DKIM para uma identidade de e-mail	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityDkimSigningAttributes	Concede permissão para configurar ou alterar as configurações de autenticação DKIM para uma identidade de domínio de e-mail	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityFeedbackAttributes	Concede permissão para ativar ou desativar o encaminhamento de feedback para uma identidade de e-mail	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutEmailIdentityMailFromAttributes	Concede permissão para habilitar ou desabilitar a configuração do domínio de MAIL FROM personalizado para uma identidade de e-mail	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutSuppressedDestination	Concede permissão para adicionar um endereço de e-mail à lista de supressão	Gravar		ses:ApiVersion	
ReplicateEmailIdentityDkimSigningKey [somente permissão]	Concede permissão para replicar a chave de assinatura DKIM da identidade de e-mail	Gerenciamento de permissões	identity*		
				ses:ReplicaRegion	
SendBulkEmail	Concede permissão para compor uma mensagem de e-mail para vários destinos	Write	identity*		
			template*		
			configuration-set		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ses:ApiVersion ses:MultiRegionEndpointId ses:TenantName	
SendCustomVerificationEmail	Concede permissão para adicionar um endereço de e-mail à lista de identidades e tenta verificá-lo	Write	custom-verification-email-template*		
				ses:ApiVersion	
SendEmail	Concede permissão para enviar uma mensagem de e-mail	Write	identity*		
			configuration-set		
			template		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients ses:MultiRegionEndpointId ses:TenantName	
TagResource	Concede permissão para adicionar uma ou mais etiquetas (chaves e valores) a um recurso especificado	Marcação	configuration-set		
			contact-list		
			dedicated-ip-pool		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			deliverability-test-report		
			identity		
			tenant		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
TestRenderEmailTemplate	Concede permissão para criar uma visualização do conteúdo MIME de um e-mail quando fornecido com um modelo e um conjunto de dados de substituição	Write	template*		
				ses:ApiVersion	
UntagResource	Concede permissão para remover uma ou mais etiquetas (chaves e valores) de um recurso especificado	Marcação	configuration-set		
			contact-list		
			dedicated-ip-pool		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			deliverability-test-report		
			identity		
			tenant		
				ses:ApiVersion aws:TagKeys	
UpdateConfigurationSetEventDestination	Concede permissão para atualizar a configuração de um destino de evento para um conjunto de configurações	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateContact	Concede permissão para atualizar as preferências de um contato para uma lista	Write	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateContactList	Concede permissão para atualizar metadados da lista de contatos	Write	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateCustomVerificationEmailTemplate	Concede permissão para atualizar um modelo de e-mail de verificação personalizado existente	Write	custom-verification-email-template*		
				ses:ApiVersion	
UpdateEmailIdentityPolicy	Concede permissão para atualizar a política de autorização de envio especificada para a determinada identidade (um endereço de e-mail ou um domínio)	Permissions management	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateEmailTemplate	Concede permissão para atualizar um modelo de e-mail	Gravar	template*		
				ses:ApiVersion	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateReputationEntityCustomerManagedStatus	Concede permissão para atualizar o status de envio gerenciado pelo cliente	Gravar	tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateReputationEntityPolicy	Concede permissão para atribuir uma política de reputação	Gravar	reputation-policy*		
			tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pelo Amazon Simple Email Service v2

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
reputation-policy	arn:${Partition}:ses:${Region}:aws:reputation-policy/${ReputationPolicyName}	
configuration-set	arn:${Partition}:ses:${Region}:${Account}:configuration-set/${ConfigurationSetName}	aws:ResourceTag/${TagKey}
contact-list	arn:${Partition}:ses:${Region}:${Account}:contact-list/${ContactListName}	aws:ResourceTag/${TagKey}
custom-verification-email-template	arn:${Partition}:ses:${Region}:${Account}:custom-verification-email-template/${TemplateName}	
dedicated-ip-pool	arn:${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}	

Tipos de recursos	ARN	Chaves de condição
template	arn:${Partition}:ses:${Region}:${Account}:template/${TemplateName}	
multi-region-endpoint	arn:${Partition}:ses:${Region}:${Account}:multi-region-endpoint/${EndpointName}	
mailmanager-archive	arn:${Partition}:ses:${Region}:${Account}:mailmanager-archive/${ArchiveId}	aws:ResourceTag/${TagKey}
tenant	arn:${Partition}:ses:${Region}:${Account}:tenant/${TenantName}/${TenantId}	aws:ResourceTag/${TagKey}

Chaves de condição para o Amazon Simple Email Service v2

O Amazon Simple Email Service v2 define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String

Chaves de condição	Descrição	Tipo
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString
ses:ApiVersion	Filtra o acesso pela versão da API do SES	String
ses:ExportSourceType	Filtra o acesso pelo tipo de origem da exportação	String
ses:FeedbackAddress	Filtra o acesso pelo endereço “Return-Path”, que especifica para onde as devoluções e reclamações são enviadas, por meio do encaminhamento de feedback de e-mail	String
ses:FromAddress	Filtra ações pelo endereço “De” de uma mensagem	String
ses:FromDisplayName	Filtra ações pelo endereço “De” que é usado como o nome de exibição de uma mensagem	String
ses:MultiRegionEndpointId	Filtra o acesso pelo ID do endpoint multirregional usado para enviar e-mails	String
ses:Recipients	Filtra ações pelos endereços de destinatários de uma mensagem que incluem os endereços “Para”, “CC” e “CCO”	ArrayOfString
ses:ReplicaRegion	Filtra o acesso pelas regiões de réplica para replicar a chave de assinatura DKIM do domínio	ArrayOfString
ses:TenantName	Filtra o acesso pelo nome do inquilino usado para enviar e-mail	String

Ações, recursos e chaves de condição do Amazon Simple Workflow Service

O Amazon Simple Workflow Service (prefixo do serviço: `swf`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Simple Workflow Service
- Tipos de recursos definidos pelo Amazon Simple Workflow Service
- Chaves de condição do Amazon Simple Workflow Service

Ações definidas pelo Amazon Simple Workflow Service

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar

a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelTimer [somente permissão]	Concede permissão para cancelar um cronômetro iniciado anteriormente e registrar um TimerCanceled evento no histórico	Gravar	domain*		
CancelWorkflowExecution [somente permissão]	Concede permissão para fechar a execução do fluxo de trabalho e registrar um WorkflowExecutionCanceled evento no histórico	Gravar	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CompleteWorkflowExecution [somente permissão]	Concede permissão para fechar a execução do fluxo de trabalho e registrar um WorkflowExecutionCompleted evento no histórico	Gravar	domain*		
ContinueAsNewWorkflowExecution [somente permissão]	Concede permissão para encerrar a execução do fluxo de trabalho e iniciar uma nova execução de fluxo de trabalho do mesmo tipo usando o mesmo ID de fluxo de trabalho e um ID de execução exclusivo	Gravar	domain*		
CountClosedWorkflowExecutions	Concede permissão para retornar o número de execuções de fluxo de trabalho encerradas no domínio específico que atendem aos critérios de filtragem especificados	Leitura	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CountOpenWorkflowExecutions	Concede permissão para retornar o número de execuções de fluxo de trabalho abertas no domínio específico que atendem aos critérios de filtragem especificados	Leitura	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	
CountPendingActivityTasks	Concede permissão para retornar o número estimado de tarefas de atividades especificadas na lista de tarefas	Leitura	domain*		
				swf:taskList.name	
CountPendingDecisionTasks	Concede permissão para retornar o número estimado de tarefas de decisão especificadas na lista de tarefas	Leitura	domain*		
				swf:taskList.name	
DeleteActivityType	Concede permissão para excluir o tipo de atividade especificado	Gravar	domain*		
				swf:activityType.name swf:activityType.version	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteWorkflowType	Concede permissão para excluir o tipo de fluxo de trabalho especificado	Gravar	domain*		
				swf:workflowType.name swf:workflowType.version	
DeprecateActivityType	Concede permissão para defasar o tipo de atividade especificado	Gravar	domain*		
				swf:activityType.name swf:activityType.version	
DeprecateDomain	Concede permissão para defasar o tipo de domínio especificado	Gravar	domain*		
DeprecateWorkflowType	Concede permissão para defasar o tipo de fluxo de trabalho especificado	Gravar	domain*		
				swf:workflowType.name swf:workflowType.version	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeActivityType	Concede permissão para retornar informações sobre o tipo de atividade especificado	Leitura	domain*		
				swf:activityType.name swf:activityType.version	
DescribeDomain	Concede permissão para retornar informações sobre o domínio especificado, inclusive a descrição e o status	Leitura	domain*		
DescribeWorkflowExecution	Concede permissão para retornar informações sobre a execução do fluxo de trabalho especificado, inclusive o tipo e algumas estatísticas	Leitura	domain*		
DescribeWorkflowType	Concede permissão para retornar informações sobre o tipo de fluxo de trabalho especificado	Leitura	domain*		
				swf:workflowType.name swf:workflowType.version	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
FailWorkflowExecution [somente permissão]	Concede permissão para fechar a execução do fluxo de trabalho e registrar um WorkflowExecutionFailed evento no histórico	Gravar	domain*		
GetWorkflowExecutionHistory	Concede permissão para retornar o histórico da execução de fluxo de trabalho especificada	Leitura	domain*		
ListActivityTypes	Concede permissão para retornar informações sobre todas as atividades registradas no domínio especificado que correspondem ao nome e status do registro especificados	Lista	domain*		
ListClosedWorkflowExecutions	Concede permissão para retornar uma lista de execuções de fluxo de trabalho encerradas no domínio especificado que atendem aos critérios de filtragem especificados	Lista	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDomains	Concede permissão para retornar a lista de domínios registrados na conta	Lista			
ListOpenWorkflowExecutions	Concede permissão para retornar uma lista de execuções de fluxo de trabalho abertas no domínio especificado que atendem aos critérios de filtragem especificados	Lista	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	
ListTagsForResource	Concede permissão para listar tags para um AWS recurso SWF	Lista	domain		
ListWorkflowTypes	Concede permissão para retornar informações sobre tipos de fluxos de trabalho no domínio especificado	Lista	domain*		
PollForActivityTask	Concede permissão aos trabalhadores para obter um ActivityTask da atividade especificada TaskList	Gravar	domain*		
				swf:taskList.name	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PollForDecisionTask	Concede permissão aos decisores para obter uma DecisionTask da decisão especificada TaskList	Gravar	domain*		
				swf:taskList.name	
RecordActivityTaskHeartbeat	Concede permissão aos trabalhadores para relatar ao serviço que o ActivityTask representado pelo TaskToken especificado ainda está progredindo	Gravar	domain*		
RecordMarker [somente permissão]	Concede permissão para gravar um MarkerRecorded evento no histórico	Gravar	domain*		
RegisterActivityType	Concede permissão para registrar um novo tipo de atividade juntamente com suas definições de configuração no domínio especificado	Gravar	domain*		
				swf:defaultTaskList.name swf:name swf:version	
RegisterDomain	Concede permissão para registrar um novo domínio	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RegisterWorkflowType	Concede permissão para registrar um novo tipo de fluxo de trabalho e suas definições de configuração no domínio especificado	Gravar	domain*		
				swf:defaultTaskList.name swf:name swf:version	
RequestCancelActivityTask [somente permissão]	Concede permissão para tentar cancelar uma tarefa de atividade anteriormente agendada	Gravar	domain*		
RequestCancelExternalWorkflowExecution [somente permissão]	Concede permissão para solicitar que seja feita uma solicitação para cancelar a execução do fluxo de trabalho externo especificado	Gravar	domain*		
RequestCancelWorkflowExecution	Concede permissão para registrar um WorkflowExecutionCancelRequested evento na execução do fluxo de trabalho atualmente em execução, identificado pelo domínio, WorkflowID e RunID fornecidos	Gravar	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RespondActivityTaskCanceled	Concede permissão aos trabalhadores para informar ao serviço que o ActivityTask identificado pelo TaskToken foi cancelado com sucesso	Gravar	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RespondActivityTaskCompleted	Concede permissão aos trabalhadores para informar ao serviço que o ActivityTask identificado pelo TaskToken foi concluído com sucesso com um resultado (se fornecido)	Gravar	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	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				swf:workflowType.name swf:workflowType.version	
RespondActivityTaskFailed	Concede permissão aos trabalhadores para informar ao serviço que o ActivityTask identificado pelo TaskToken falhou por um motivo (se especificado)	Gravar	domain*		
RespondDecisionTaskCompleted	Concede permissão aos decisores para informar ao serviço que o DecisionTask identificado pelo TaskToken foi concluído com êxito	Gravar	domain*		
ScheduleActivityTask [somente permissão]	Concede permissão para agendar uma tarefa de atividade	Gravar	domain*		
SignalExternalWorkflowExecution [somente permissão]	Concede permissão para solicitar o envio de um sinal à execução especificada do fluxo de trabalho externo e os registros	Gravar	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SignalWorkflowExecution	Concede permissão para registrar um WorkflowExecutionSignaled evento no histórico de execução do fluxo de trabalho e criar uma tarefa de decisão para a execução do fluxo de trabalho identificada pelo domínio determinado, WorkflowID e RunID	Gravar	domain*		
StartChildWorkflowExecution [somente permissão]	Concede permissão para solicitar o início de uma execução de fluxo de trabalho filho	Gravar	domain*		
StartTimer [somente permissão]	Concede permissão para iniciar um timer para uma execução de fluxo de trabalho	Gravar	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartWorkflowExecution	Concede permissão para iniciar uma execução do tipo de fluxo de trabalho no domínio especificado usando os workflowId e os dados de entrada fornecidos	Gravar	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	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para marcar um recurso AWS SWF	Tags	domain		
				aws:TagKeys aws:RequestTag/${TagKey}	
TerminateWorkflowExecution	Concede permissão para registrar um WorkflowExecutionTerminated evento e forçar o encerramento da execução do fluxo de trabalho identificada pelo domínio, RunID e WorkflowID fornecidos	Gravar	domain*		
UndeprecateActivityType	Concede permissão para cancelar a defasagem de um tipo de atividade defasada anteriormente	Gravar	domain*		
				swf:activityType.name swf:activityType.version	
UndeprecateDomain	Concede permissão para cancelar a defasagem de um domínio anteriormente defasado	Gravar	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UndeprecateWorkflowType	Concede permissão para cancelar a defasagem de um tipo de fluxo de trabalho anteriormente defasado	Gravar	domain*		
				swf:workflowType.name swf:workflowType.version	
UntagResource	Concede permissão para remover uma tag de um recurso AWS SWF	Tags	domain		
				aws:TagKeys	

Tipos de recursos definidos pelo Amazon Simple Workflow Service

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
domain	`arn:${Partition}:swf::${Account}:/domain/${DomainName}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Simple Workflow Service

O Amazon Simple Workflow Service define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por etiqueta da solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por etiqueta do recurso	String
aws:TagKeys	Filtra o acesso por etiqueta da chave	ArrayOfString
swf:activityType.name	Filtra o acesso pelo nome do tipo da atividade	String
swf:activityType.version	Filtra o acesso pela versão do tipo da atividade	String
swf:defaultTaskList.name	Filtra o acesso pelo nome da lista de tarefas padrão	String
swf:name	Filtra o acesso pelo nome de atividades ou fluxos de trabalho	String
swf:tagFilter.tag	Filtra o acesso pelo valor de tagFilter.tag	String
swf:tagList.member.0	Filtra o acesso pela etiqueta especificada	String

Chaves de condição	Descrição	Tipo
swf:tagList.member.1	Filtra o acesso pela etiqueta especificada	String
swf:tagList.member.2	Filtra o acesso pela etiqueta especificada	String
swf:tagList.member.3	Filtra o acesso pela etiqueta especificada	String
swf:tagList.member.4	Filtra o acesso pela etiqueta especificada	String
swf:taskList.name	Filtra o acesso pelo nome da lista de tarefas	String
swf:typeFilter.name	Filtra o acesso pelo nome do filtro de tipos	String
swf:typeFilter.version	Filtra o acesso pela versão do filtro de tipos	String
swf:version	Filtra o acesso pela versão de atividades ou fluxos de trabalho	String
swf:workflowType.name	Filtra o acesso pelo nome do tipo de fluxo de trabalho	String
swf:workflowType.version	Filtra o acesso pela versão do tipo de fluxo de trabalho	String

Ações, recursos e chaves de condição do Amazon SimpleDB

O Amazon SimpleDB (prefixo do serviço: `sdb`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon SimpleDB
- Tipos de recursos definidos pelo Amazon SimpleDB
- Chaves de condição do Amazon SimpleDB

Ações definidas pelo Amazon SimpleDB

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de

condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchDeleteAttributes	Executa várias DeleteAttributes operações em uma única chamada, o que reduz as viagens de ida e volta e as latências	Gravar	domain*		
BatchPutAttributes	Com a BatchPutAttributes operação, você pode realizar várias PutAttribute operações em uma única chamada. Com a BatchPutAttributes operação, você pode realizar várias PutAttribute operações em uma única chamada	Gravar	domain*		
CreateDomain	A CreateDomain operação cria um novo domínio	Gravar	domain*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteAttributes	Exclui um ou mais atributos associados ao item	Gravar	domain*		
DeleteDomain	A DeleteDomain operação exclui um domínio	Gravar	domain*		
DomainMetadata	Retorna informações sobre o domínio incluindo quando o domínio foi criado, o número de itens e atributos, o tamanho dos nomes e os valores dos atributos	Leitura	domain*		
GetAttributes	Retorna todos os atributos associados ao item	Leitura	domain*		
ListDomains	Descrição para ListDomains	Lista			
PutAttributes	A PutAttributes operação cria ou substitui atributos em um item	Gravar	domain*		
Select	Descrição de Select	Read	domain*		

Tipos de recursos definidos pelo Amazon SimpleDB

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
domain	`arn:${Partition}:sdb:${Region}:${Account}:domain/${DomainName}`	

Chaves de condição do Amazon SimpleDB

O SimpleDB não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para AWS SimSpace Weaver

AWS SimSpace O Weaver (prefixo do serviço:`simspaceweaver`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS SimSpace Weaver
- Tipos de recursos definidos pelo AWS SimSpace Weaver
- Chaves de condição para AWS SimSpace Weaver

Ações definidas pelo AWS SimSpace Weaver

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSnapshot	Concede permissão para criar um snapshot	Gravar	Simulation*		
DeleteApp	Concede permissão para excluir uma aplicação	Gravar	Simulation*		
DeleteSimulation	Concede permissão para excluir uma simulação	Gravar	Simulation*		
DescribeApp	Concede permissão para descrever uma aplicação	Leitura	Simulation*		
DescribeSimulation	Concede permissão para descrever uma simulação	Leitura	Simulation*		
ListApps	Concede permissão para listar aplicações	Leitura	Simulation*		
ListSimulations	Concede permissão para listar simulações	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura			
StartApp	Concede permissão para iniciar uma aplicação	Gravar	Simulation*		
StartClock	Concede permissão para iniciar uma simulação de relógio	Gravar	Simulation*		
StartSimulation	Concede permissão para iniciar uma simulação	Gravar		aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
StopApp	Concede permissão para interromper uma aplicação	Gravar	Simulation*		
StopClock	Concede permissão para interromper uma simulação de relógio	Gravar	Simulation*		
StopSimulation	Concede permissão para interromper uma simulação	Gravar	Simulation*		
TagResource	Concede permissão para marcar um recurso	Marcação	Simulation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso	Tags	Simulation*		
				aws:TagKeys	

Tipos de recursos definidos pelo AWS SimSpace Weaver

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso

também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
Simulation	`arn:${Partition}:simspaceweaver:${Region}:${Account}:simulation/${SimulationName}`	aws:ResourceTag/${TagKey}

Chaves de condição para AWS SimSpace Weaver

AWS SimSpace O Weaver define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves de etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS Snow Device Management

AWS O Snow Device Management (prefixo do serviço:`snow-device-management`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Snow Device Management
- Tipos de recurso definidos pelo AWS Snow Device Management
- Chaves de condição para o AWS Snow Device Management

Ações definidas pelo AWS Snow Device Management

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar

a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelTask	Concede permissão para cancelar tarefas em dispositivos remotos	Gravar	task*		
CreateTask	Concede permissão para criar tarefas em dispositivos remotos	Gravar		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
DescribeDevice	Concede permissão para descrever um dispositivo gerenciado remotamente	Leitura	managed-device*		
DescribeDeviceEc2Instances	Concede permissão para descrever as instâncias de um dispositivo gerenciado remotamente EC2	Leitura	managed-device*		
DescribeExecution	Concede permissão para descrever execuções de tarefas	Leitura			
DescribeTask	Concede permissão para descrever uma tarefa	Leitura	task*		
ListDeviceResources	Concede permissão para listar os recursos de um dispositivo gerenciado remotamente	Lista	managed-device*		
ListDevices	Concede permissão para listar os dispositivos gerenciados remotamente	Lista			
ListExecutions	Concede permissão para listar as execuções de tarefa	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso (dispositivo ou tarefa)	Leitura		aws:RequestTag/${TagKey} aws:TagKeys	
ListTasks	Concede permissão para listar tarefas	Lista			
TagResource	Concede permissão para marcar um recurso	Marcação	managed-device		
			task		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso	Tags	managed-device		
			task		
				aws:TagKeys	

Tipos de recurso definidos pelo AWS Snow Device Management

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações

identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição para o AWS Snow Device Management

AWS O Snow Device Management define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso pela chave e valor de uma etiqueta em uma solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pela presença de pares chave-valor da etiqueta anexados ao recurso	Segmento

Chaves de condição	Descrição	Type
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Snowball

AWS O Snowball (prefixo do serviço:`snowball`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Snowball
- Tipos de recursos definidos pelo AWS Snowball
- Chaves de condição do AWS Snowball

Ações definidas pelo AWS Snowball

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelCluster	Concede permissão para cancelar um trabalho de cluster	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelJob	Concede permissão para cancelar o trabalho especificado	Gravar			
CreateAddress	Concede permissão para criar um endereço para o qual enviar um Snowball	Gravar			
CreateCluster	Concede permissão para criar um cluster vazio	Gravar			
CreateJob	Concede permissão para criar um trabalho para importar ou exportar dados entre o Amazon S3 e o datacenter on-premises	Gravar			
CreateLongTermPricing	Concede permissão para criar um LongTermPricingListEntry para permitir que os clientes adicionem um contrato de cobrança antecipada para um trabalho	Gravar			
CreateReturnShippingLabel	Concede permissão para criar uma etiqueta de remessa que será usada para devolver o dispositivo Snow para AWS	Gravar			
DescribeAddress	Concede permissão para obter detalhes específicos sobre o endereço na forma de um objeto de Address	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeAddresses	Concede permissão para descrever um número especificado de objetos ADDRESS	Lista			
DescribeCluster	Concede permissão para descrever informações sobre um cluster específico, incluindo informações sobre envio, status do cluster e outros metadados importantes	Leitura			
DescribeJob	Concede permissão para descrever informações sobre um trabalho específico, incluindo informações sobre envio, status do trabalho e outros metadados importantes	Leitura			
DescribeReturnShippingLabel	Concede permissão para descrever informações na etiqueta de remessa de um dispositivo Snow que está sendo devolvido para AWS	Leitura			
GetJobManifest	Concede permissão para obter um link para uma URL pré-assinada do Amazon S3 para o arquivo de manifesto associado ao valor especificado JobId	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetJobUnlockCode	Concede permissão para obter o valor UnlockCode do código para o trabalho especificado	Leitura			
GetSnowballUsage	Concede permissão para obter informações sobre o limite do serviço Snowball para sua conta, e também o número de Snowballs que sua conta tem em uso	Leitura			
GetSoftwareUpdates	Concede permissão para retornar uma URL pré-assinada do Amazon S3 para um arquivo de atualização associado a um determinado JobId	Leitura			
ListClusterJobs	Concede permissão para listar JobListEntry objetos do tamanho especificado	Lista			
ListClusters	Concede permissão para listar ClusterListEntry objetos do tamanho especificado	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListCompatibleImages	Concede permissão para retornar uma lista das diferentes Amazon EC2 Amazon Machine Images (AMIs) de sua propriedade e Conta da AWS que seriam suportadas para uso em um dispositivo Snow	Lista			
ListJobs	Concede permissão para listar JobListEntry objetos do tamanho especificado	Lista			
ListLongTermPricing	Concede permissão para listar LongTermPricingListEntry objetos para a conta que está fazendo a solicitação	Leitura			
ListPickupLocations	Concede permissão para listar objetos de endereço onde a coleta está disponível, com o comprimento especificado	Lista			
ListServiceVersions	Concede permissão para listar todas as versões compatíveis com serviços do Snow no dispositivo	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateCluster	Concede permissão para atualização. Enquanto o ClusterState valor de um cluster está no AwaitingQuorum estado, você pode atualizar algumas das informações associadas a um cluster	Gravar			
UpdateJob	Concede permissão para atualização. Embora o JobState valor de um trabalho seja Novo, você pode atualizar algumas das informações associadas a um trabalho	Gravar			
UpdateJobShipmentState	Concede permissão para atualizar o estado quando um dos estados de envio é alterado para outro estado	Gravar			
UpdateLongTermPricing	Concede permissão para atualizar um contrato de cobrança inicial específico para um trabalho	Gravar			

Tipos de recursos definidos pelo AWS Snowball

AWS O Snowball não suporta a especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para conceder acesso ao AWS Snowball, especifique `"Resource": "*"` na política.

Chaves de condição do AWS Snowball

O Snowball não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do Amazon SNS

O Amazon SNS (prefixo do serviço: `sns`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon SNS
- Tipos de recursos definidos pelo Amazon SNS
- Chaves de condição do Amazon SNS

Ações definidas pelo Amazon SNS

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos

("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddPermission	Concede permissão para adicionar uma declaração à política de controle de acesso de um tópico, concedendo acesso às ações especificadas para as AWS contas especificadas	Gerenciamento de permissões	topic*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CheckIfPhoneNumberIsOptedOut	Concede permissão para aceitar um número de telefone e indicar se o titular do telefone cancelou a opção de recebimento de mensagens SMS em sua conta	Read			
ConfirmSubscription	Concede permissão para verificar a intenção do proprietário de um endpoint de receber mensagens validando o token enviado para o endpoint por uma ação Subscribe anterior	Write	topic*		
CreatePlatformApplication	Concede permissão para criar um objeto de aplicação de plataforma para um dos serviços de notificações por push compatíveis, como APNS e GCM, nos quais dispositivos e aplicativos móveis podem ser inscritos	Write			iam:PassRole
CreatePlatformEndpoint	Concede permissão para criar um endpoint para um dispositivo e aplicativo móvel em um dos serviços de notificações por push compatíveis, como GCM e APNS	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSMSSandboxPhoneNumber	Concede permissão para adicionar um número de telefone de destino e enviar uma senha de uso único (OTP) a esse número de telefone para um Conta da AWS	Gravar			
CreateTopic	Concede permissão para criar um tópico no qual as notificações possam ser publicadas	Write	topic*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteEndpoint	Concede permissão para excluir o endpoint de um dispositivo e aplicativo móvel do Amazon SNS	Write			
DeletePlatformApplication	Concede permissão para excluir um objeto de aplicação da plataforma de um dos serviços de notificações por push compatíveis, como APNS e GCM	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteSMSSandboxPhoneNumber	Concede permissão para excluir um número Conta da AWS de telefone verificado ou pendente	Gravar			
DeleteTopic	Concede permissão para excluir um tópico e todas as suas assinaturas	Gravar	topic*		
GetDataProtectionPolicy	Concede permissão para retornar a política de proteção de dados do tópico	Leitura	topic*		
GetEndpointAttributes	Concede permissão para recuperar os atributos do endpoint de um dispositivo em um dos serviços de notificações por push compatíveis, como GCM e APNS	Read			
GetPlatformApplicationAttributes	Concede permissão para recuperar os atributos do objeto de aplicação da plataforma dos serviços de notificações por push compatíveis, como APNS e GCM	Read			
GetSMSAttributes	Concede permissão para retornar as configurações de envio de mensagens SMS da sua conta	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSMSSandboxAccountStatus	Concede permissão para recuperar o status da sandbox para a conta de chamada na região de destino	Read			
GetSubscriptionAttributes	Concede permissão para retornar todas as propriedades de uma assinatura	Read			
GetTopicAttributes	Concede permissão para retornar todas as propriedades de um tópico	Read	topic*		
ListEndpointsByPlatformApplication	Concede permissão para relacionar os endpoints e os atributos dos endpoints de dispositivos em um serviço de notificações por push compatível, como GCM e APNS	List			
ListOriginationNumbers	Concede permissão para relacionar todos os números de origem e seus metadados	List			
ListPhoneNumbersOptedOut	Concede permissão para retornar uma lista de números de telefone cancelados, o que significa que você não pode enviar mensagens SMS a eles	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListPlatformApplications	Concede permissão para relacionar os objetos de aplicação da plataforma dos serviços de notificações por push compatíveis, como APNS e GCM	List			
ListSMSSandboxPhoneNumbers	Concede permissão para os números de telefone de destino atuais, pendentes e verificados, da conta de chamada	List			
ListSubscriptions	Concede permissão para retornar uma lista das assinaturas do solicitante	List			
ListSubscriptionsByTopic	Concede permissão para retornar uma lista das inscrições para um determinado tópico	List	topic*		
ListTagsForResource	Concede permissão para relacionar todas as etiquetas adicionadas ao tópico especificado do Amazon SNS	Read	topic		
ListTopics	Concede permissão para retornar uma lista dos tópicos do solicitante	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
OptInPhoneNumber	Concede permissão para aceitar um número de telefone que está cancelado no momento, o que permite que você retome o envio de mensagens SMS para o número.	Write			
Publish	Concede permissão para enviar uma mensagem para todos os endpoints inscritos de um tópico	Gravar	topic*		
PutDataProtectionPolicy	Concede permissão para autorizar um proprietário de tópico a definir a política de proteção de dados	Gravar	topic*		
RemovePermission	Concede permissão para remover uma instrução da política de controle de acesso de um tópico	Permissions management	topic*		
SetEndpointAttributes	Concede permissão para definir os atributos de um endpoint de um dispositivo em um dos serviços de notificações por push compatíveis, como GCM e APNS	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SetPlatformApplicationAttributes	Concede permissão para definir os atributos do objeto de aplicação da plataforma dos serviços de notificações por push compatíveis, como APNS e GCM	Write			iam:PassRole
SetSMSAttributes	Concede permissão para definir as configurações padrão para enviar mensagens SMS e receber relatórios diários de uso de SMS	Write			
SetSubscriptionAttributes	Concede permissão para permitir que um proprietário da assinatura defina um atributo do tópico para um novo valor	Write			
SetTopicAttributes	Concede permissão para permitir que um proprietário de tópico defina um atributo do tópico para um novo valor	Gerenciamento de permissões	topic*		iam:PassRole
Subscribe	Concede permissão para se preparar para assinar um endpoint por meio do envio de uma mensagem de confirmação a ele	Write	topic*		
				sns:Endpoint sns:Protocol	
TagResource		Marcação	topic		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	Concede permissão para adicionar etiquetas ao tópico especificado do Amazon SNS			aws:RequestTag/${TagKey} aws:TagKeys	
Unsubscribe	Concede permissão para excluir uma assinatura	Write			
UntagResource	Concede permissão para remover as etiquetas do tópico do Amazon SNS especificado	Tags	topic		
				aws:TagKeys	
VerifySMSSandboxPhoneNumber	Concede permissão para verificar um número de telefone de destino com uma senha de uso único (OTP) para um Conta da AWS	Gravar			

Tipos de recursos definidos pelo Amazon SNS

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
topic	`arn:${Partition}:sns:${Region}:${Account}:${TopicName}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon SNS

O Amazon SNS define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso baseado em etiquetas a partir da solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra o acesso baseado nas chaves da etiqueta a partir da solicitação	ArrayOfString
sns:Endpoint	Filtra o acesso com base no URL, no endereço de e-mail ou no ARN de uma solicitação de assinatura ou de uma assinatura confirmada anteriormente	String
sns:Protocol	Filtra o acesso com base no valor do protocolo de uma solicitação de assinatura ou de uma assinatura confirmada anteriormente	String

Ações, recursos e chaves de condição para o AWS SQL Workbench

AWS O SQL Workbench (prefixo do serviço:`sqlworkbench`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS SQL Workbench
- Tipos de recursos definidos pelo AWS SQL Workbench
- Chaves de condição do AWS SQL Workbench

Ações definidas pelo AWS SQL Workbench

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateConnectionWithChart [somente permissão]	Concede permissão para associar uma conexão a um gráfico	Gravar	chart* connection*		
AssociateConnectionWithTab [somente permissão]	Concede permissão para associar uma conexão a uma guia	Gravar	connection*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateNotebookWithTab [somente permissão]	Concede permissão para associar um caderno a uma guia	Gravar	notebook*		
AssociateQueryWithTab [somente permissão]	Concede permissão para associar uma consulta a uma guia	Gravar	query*		
BatchDeleteFolder [somente permissão]	Concede permissão para excluir pastas em sua conta	Gravar			
BatchGetNotebookCell [somente permissão]	Concede permissão para obter células de bloco de anotações em sua conta	Leitura	notebook*		
CreateAccount [somente permissão]	Concede permissão para criar uma SQLWorkbench conta	Gravar			
CreateChart [somente permissão]	Concede permissão para criar um novo gráfico salvo em sua conta	Gravar	chart*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateConnection [somente permissão]	Concede permissão para criar uma nova conexão na sua conta	Gravar	connection*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateFolder [somente permissão]	Concede permissão para criar uma pasta na sua conta	Gravar			
CreateNotebook [somente permissão]	Concede permissão para criar um novo bloco de anotações em sua conta	Gravar	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateNotebookCell [somente permissão]	Concede permissão para criar uma célula de bloco de anotações em sua conta	Gravar	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateNotebookFromVersion [somente permissão]	Concede permissão para criar um novo bloco de anotações com base em uma versão de bloco de anotações de sua conta	Gravar	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateNotebookVersion [somente permissão]	Concede permissão para criar uma versão de bloco de anotações em sua conta	Gravar	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateSavedQuery [somente permissão]	Concede permissão para criar uma nova consulta salva na sua conta	Gravar	query*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteChart [somente permissão]	Concede permissão para remover gráficos na sua conta	Gravar	chart*		
DeleteConnection [somente permissão]	Concede permissão para remover conexões na sua conta	Gravar	connection*		
DeleteNotebook [somente permissão]	Concede permissão para remover blocos de anotações de sua conta	Gravar	notebook*		
DeleteNotebookCell [somente permissão]	Concede permissão para remover células de bloco de anotações de sua conta	Gravar	notebook*		
DeleteNotebookVersion [somente permissão]	Concede permissão para remover células de bloco de anotações de sua conta	Gravar	notebook*		
DeleteQCustomContext [somente permissão]	Concede permissão para excluir o contexto personalizado de toda a conta	Gravar			
DeleteSavedQuery [somente permissão]	Concede permissão para remover consultas salvas na sua conta	Gravar	query*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteSqlGenerationContext [somente permissão]	Concede permissão para excluir o contexto de geração de sql	Gravar			
DeleteTab [somente permissão]	Concede permissão para remover uma guia da sua conta	Gravar			
DriverExecute [somente permissão]	Concede permissão para executar uma consulta em seu cluster de redshift	Gravar	connection*		
DuplicateNotebook [somente permissão]	Concede permissão para criar um bloco de anotações duplicando um existente em sua conta	Gravar	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ExportNotebook [somente permissão]	Concede permissão para exportar um bloco de anotações de sua conta	Leitura	notebook*		
GenerateSession [somente permissão]	Concede permissão para gerar uma nova sessão na sua conta	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAccountInfo [somente permissão]	Concede permissão para obter informações da conta	Leitura			
GetAccountSettings [somente permissão]	Concede permissão para obter configurações da conta	Leitura			
GetAutocompletionMetadata [somente permissão]	Concede permissão para obter metadados da estrutura do banco de dados para preenchimento automático	Leitura			
GetAutocompletionResource [somente permissão]	Concede permissão para obter informações da estrutura do banco de dados para preenchimento automático	Leitura			
GetChart [somente permissão]	Concede permissão para obter gráficos na sua conta	Leitura	chart*		
GetConnection [somente permissão]	Concede permissão para obter conexões na sua conta	Leitura	connection*		
GetNotebook [somente permissão]	Concede permissão para obter metadados de bloco de anotações em sua conta	Leitura	notebook*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetNotebookVersion [somente permissão]	Concede permissão para obter o conteúdo de uma versão de bloco de anotações em sua conta	Leitura	notebook*		
GetQCustomContext [somente permissão]	Concede permissão para obter contexto personalizado em toda a conta	Leitura			
GetQSqlPromptQuotas [somente permissão]	Concede permissão para obter cotas máximas de prompt do SQL generativo do Q	Leitura			
GetQSqlRecommendations [somente permissão]	Concede permissão para obter recomendações de texto para SQL	Leitura			
GetQueryExecutionHistory [somente permissão]	Concede permissão para obter o histórico de execução da consulta na sua conta	Leitura			
GetSavedQuery [somente permissão]	Concede permissão para obter consultas salvas em sua conta	Leitura	query*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSchemaInference [somente permissão]	Concede permissão para obter as colunas e os tipos de dados inferidos de um arquivo	Leitura			
GetSqlGenerationContext [somente permissão]	Concede permissão para obter o contexto de geração de sql	Leitura			
GetSqlRecommendations [somente permissão]	Concede permissão para obter recomendações de texto para SQL	Leitura			
GetUserInfo [somente permissão]	Concede permissão para obter informações do usuário	Leitura			
GetUserWorkspaceSettings [somente permissão]	Concede permissão para obter as configurações de workspace na sua conta	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ImportNotebook [somente permissão]	Concede permissão para importar um bloco de anotações para sua conta	Gravar	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ListConnections [somente permissão]	Concede permissão para listar as conexões na sua conta	Listar			
ListDatabases [somente permissão]	Concede permissão para listar bancos de dados do seu cluster de redshift	Lista			
ListFiles [somente permissão]	Concede permissão para listar arquivos e pastas	Lista			
ListNotebookVersions [somente permissão]	Concede permissão para obter versões de metadados de bloco de anotações em sua conta	Lista	notebook*		
ListNotebooks [somente permissão]	Concede permissão para listar os blocos de anotação de sua conta	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListQueryExecutionHistory [somente permissão]	Concede permissão para listar o histórico de execução da consulta na sua conta	Lista			
ListRedshiftClusters [somente permissão]	Concede permissão para listar clusters de redshift na sua conta	Lista			
ListSampleDatabases [somente permissão]	Concede permissão para listar bancos de dados	Leitura			
ListSavedQueryVersions [somente permissão]	Concede permissão para listar versões da consulta salva na sua conta	Lista	query*		
ListTabs [somente permissão]	Concede permissão para listar guias na sua conta	Lista			
ListTaggedResources [somente permissão]	Concede permissão para listar recursos marcados	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource [somente permissão]	Concede permissão para listar as etiquetas de um recurso sqlworkbench	Leitura	chart		
			connection		
			notebook		
			query		
PassAccountSettings [somente permissão]	Concede permissão para fornecer configurações de conta com a solicitação	Gravar			
PutQCustomContext [somente permissão]	Concede permissão para atualizar o contexto personalizado em toda a conta	Gravar			
PutSqlGenerationContext [somente permissão]	Concede permissão para atualizar o contexto de geração de sql	Gravar			
PutTab [somente permissão]	Concede permissão para criar ou atualizar uma guia da sua conta	Gravar			
PutUserWorkspaceSettings [somente permissão]	Concede permissão para atualizar as configurações de workspace na sua conta	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RestoreNotebookVersion [somente permissão]	Concede permissão para restaurar um bloco de anotações em sua conta para uma versão	Gravar	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagResource [somente permissão]	Concede permissão para etiquetar um recurso sqlworkbench	Tags	chart		
			connection		
			notebook		
			query		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [somente permissão]	Concede permissão para desetiquetar um recurso sqlworkbench	Tags	chart		
			connection		
			notebook		
			query		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
UpdateAccountConnectionSettings [somente permissão]	Concede permissão para atualizar as configurações de conexão em toda a conta	Gravar			
UpdateAccountExportSettings [somente permissão]	Concede permissão para atualizar as configurações de exportação em toda a conta	Gravar			
UpdateAccountGeneralSettings [somente permissão]	Concede permissão para atualizar configurações gerais de toda a conta	Gravar			
UpdateAccountQSqlSettings [somente permissão]	Concede permissão para atualizar as configurações de texto para SQL em toda a conta	Gravar			
UpdateChart [somente permissão]	Concede permissões para atualizar um gráfico na sua conta	Gravar	chart*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateConnection [somente permissão]	Concede permissão para atualizar uma conexão na sua conta	Gravar	connection*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateFileFolder [somente permissão]	Concede permissão para mover arquivos na sua conta	Gravar	chart		
			query		
UpdateFolder [somente permissão]	Concede permissão para atualizar o nome e os detalhes de uma pasta na sua conta	Gravar			
UpdateNotebook [somente permissão]	Concede permissão para atualizar metadados de um bloco de anotações em sua conta	Gravar	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateNotebookCellContent [somente permissão]	Concede permissão para atualizar o conteúdo de uma célula de bloco de anotações em sua conta	Gravar	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateNotebookCellLayout [somente permissão]	Concede permissão para atualizar um layout de célula de bloco de anotações em sua conta	Gravar	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateSavedQuery [somente permissão]	Concede permissão para atualizar uma consulta salva na sua conta	Gravar	query*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Tipos de recursos definidos pelo AWS SQL Workbench

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves

são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS SQL Workbench

AWS O SQL Workbench define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas que estão associadas ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon SQS

O Amazon SQS (prefixo do serviço: `sqs`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon SQS
- Tipos de recursos definidos pelo Amazon SQS
- Chaves de condição do Amazon SQS

Ações definidas pelo Amazon SQS

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddPermission	Concede permissão para uma fila para uma determinada entidade principal	Gerenciamento de permissões	queue*		
CancelMessageMoveTask	Concede permissão para cancelar uma tarefa de movimentação de mensagem em andamento	Gravar	queue*		
ChangeMessageVisibility	Concede permissão para alterar o tempo limite de visibilidade de uma mensagem especificada em uma fila para um novo valor	Gravar	queue*		
CreateQueue	Concede permissão para criar uma nova fila ou retorna a URL de uma fila existente	Gravar	queue*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteMessage	Concede permissão para excluir a mensagem especificada da fila especificada	Gravar	queue*		
DeleteQueue	Concede permissão para excluir a fila especificada pela URL da fila, independentemente de a fila estar vazia	Gravar	queue*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetQueueAttributes	Concede permissão para obter atributos da fila especificada	Leitura	queue*		
GetQueueUrl	Concede permissão para retornar a URL de uma fila existente	Leitura	queue*		
ListDeadLetterSourceQueues	Concede permissão para retornar uma lista de suas filas que têm o atributo RedrivePolicy queue configurado com uma fila de letras mortas	Leitura	queue*		
ListMessageMoveTasks	Concede permissão para listar tarefas de movimentação de mensagem	Leitura	queue*		
ListQueueTags	Concede permissão para listar etiquetas adicionadas a uma fila do SQS	Leitura	queue*		
ListQueues	Concede permissão para retornar uma lista de suas filas	Leitura			
PurgeQueue	Concede permissão para excluir as mensagens em uma fila especificada pela URL da fila	Gravar	queue*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ReceiveMessage	Concede permissão para recuperar uma ou mais mensagens, com um limite máximo de 10 mensagens, da fila especificada	Leitura	queue*		
RemovePermission	Concede permissão para revogar todas permissões na política de fila que corresponde ao parâmetro Label especificado	Gerenciamento de permissões	queue*		
SendMessage	Concede permissão para entregar uma mensagem para a fila especificada	Gravar	queue*		
SetQueueAttributes	Concede permissão para definir o valor de um ou mais atributos da fila	Gravar	queue*		
StartMessageMoveTask	Concede permissão para iniciar uma tarefa de movimentação de mensagem	Gravar	queue*		
TagQueue	Concede permissão para adicionar etiquetas à fila SQS especificada	Tags	queue*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagQueue	Concede permissão para remover as etiquetas da fila SQS especificada	Tags	queue*		
				aws:TagKeys	

Tipos de recursos definidos pelo Amazon SQS

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

> **Note**
>
> O ARN da fila é usado apenas em políticas de permissões do IAM. Nas chamadas à API e à CLI, você usa a URL da fila.

Tipos de recursos	ARN	Chaves de condição
queue	`arn:${Partition}:sqs:${Region}:${Account}:${QueueName}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon SQS

O Amazon SQS define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as

condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Step Functions

AWS Step Functions (prefixo do serviço:`states`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Step Functions
- Tipos de recursos definidos pelo AWS Step Functions
- Chaves de condição do AWS Step Functions

Ações definidas pelo AWS Step Functions

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateActivity	Concede permissão para criar uma atividade	Write	activity*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStateMachine	Concede permissão para criar uma máquina de estado	Gravar	statemachine*		iam:PassRole states:PublishStateMachineVersion
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStateMachineAlias	Concede permissão para criar um alias de uma máquina de estado	Gravar	statemachine*		
				states:StateMachineQualifier	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteActivity	Concede permissão para excluir uma atividade	Write	activity*		
DeleteStateMachine	Concede permissão para excluir uma máquina de estado	Gravar	statemachine*		
DeleteStateMachineAlias	Concede permissão para excluir um alias de uma máquina de estado	Gravar	statemachine*		
				states:StateMachineQualifier	
DeleteStateMachineVersion	Concede permissão para excluir uma versão de uma máquina de estado	Gravar	statemachine*		
				states:StateMachineQualifier	
DescribeActivity	Concede permissão para descrever uma atividade	Read	activity*		
DescribeExecution	Concede permissão para descrever uma execução	Leitura	execution*		
			express*		
DescribeMapRun	Concede permissão para descrever uma execução de mapa	Leitura	maprun*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeStateMachine	Concede permissão para descrever uma máquina de estado	Leitura	statemachine*		
				states:StateMachineQualifier	
DescribeStateMachineAlias	Concede permissão para descrever um alias de uma máquina de estado	Leitura	statemachine*		
				states:StateMachineQualifier	
DescribeStateMachineForExecution	Concede permissão para descrever a máquina de estado para uma execução	Read	execution*		
GetActivityTask	Concede permissão a ser usada pelos funcionários para recuperar uma tarefa (com o ARN de atividade especificada) que foi programada para execução por uma máquina de estado em execução	Write	activity*		
GetExecutionHistory	Concede permissão para retornar o histórico da execução especificada como uma lista de eventos	Leitura	execution*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
InvokeHTTPEndpoint [somente permissão]	Concede permissão para invocar o estado Tarefa de HTTP	Gravar			
ListActivities	Concede permissão para listar as atividades existentes	List			
ListExecutions	Concede permissão para listar as execuções de uma máquina de estado	Lista	maprun*		
			statemachine*		
				states:StateMachineQualifier	
ListMapRuns	Concede permissão para listar as execuções de um mapa em uma execução	Lista	execution*		
ListStateMachineAliases	Concede permissão para listar os aliases de uma máquina de estado	Lista	statemachine*		
				states:StateMachineQualifier	
ListStateMachineVersions	Concede permissão para listar as versões de uma máquina de estado	Lista	statemachine*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListStateMachines	Concede permissão para lista as máquinas de estado existentes	Lista			
ListTagsForResource	Concede permissão para listar tags para um recurso AWS Step Functions	Lista	activity statemachine		
PublishStateMachineVersion	Concede permissão para publicar uma versão de estado de máquina	Gravar	statemachine*		
RedriveExecution	Concede permissão para redirecionar uma execução	Gravar	execution*		
RevealSecrets [somente permissão]	Concede permissão para revelar dados confidenciais de uma execução	Leitura			
SendTaskFailure	Concede permissão para informar que a tarefa identificada pelo taskToken falhou	Write			
SendTaskHeartbeat	Concede permissão para informar ao serviço que a tarefa representada pelo taskToken especificado ainda está progredindo	Write			
SendTaskSuccess	Concede permissão para informar que a tarefa identificada pelo taskToken foi concluída com êxito	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartExecution	Concede permissão para iniciar uma execução de máquina de estado	Write	statemachine*		
				states:StateMachineQualifier	
StartSyncExecution	Concede permissão para iniciar uma execução de máquina de estado Synchronous Express	Write	statemachine*		
				states:StateMachineQualifier	
StopExecution	Concede permissão para interromper uma execução	Gravar	execution*		
TagResource	Concede permissão para marcar um recurso AWS Step Functions	Tags	activity		
			statemachine		
				aws:TagKeys aws:RequestTag/${TagKey}	
TestState	Concede permissão para testar uma definição de máquina de estados	Gravar			states:RevealSecrets
UntagResource		Tags	activity		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	Concede permissão para remover uma tag de um recurso AWS Step Functions		statemachine		
				aws:TagKeys	
UpdateMapRun	Concede permissão para atualizar uma execução de mapa	Gravar	maprun*		
UpdateStateMachine	Concede permissão para atualizar uma máquina de estado	Gravar	statemachine*		iam:PassRole states:PublishStateMachineVersion
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateStateMachineAlias	Concede permissão para atualizar um alias de uma máquina de estado	Gravar	statemachine*		
				states:StateMachineQualifier	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ValidateStateMachineDefinition	Concede permissão para validar uma definição de máquina de estados	Leitura			

Tipos de recursos definidos pelo AWS Step Functions

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Tipos de recursos	ARN	Chaves de condição
statemachineversion	`arn:${Partition}:states:${Region}:${Account}:stateMachine:${StateMachineName}:${StateMachineVersionId}`	aws:ResourceTag/${TagKey}
statemachinealias	`arn:${Partition}:states:${Region}:${Account}:stateMachine:${StateMachineName}:${StateMachineAliasName}`	aws:ResourceTag/${TagKey}
maprun	`arn:${Partition}:states:${Region}:${Account}:mapRun:${StateMachineName}/${MapRunLabel}:${MapRunId}`	
labelledexecution	`arn:${Partition}:states:${Region}:${Account}:execution:${StateMachineName}/${MapRunLabel}:${ExecutionId}`	
labelledexpress	`arn:${Partition}:states:${Region}:${Account}:express:${StateMachineName}/${MapRunLabel}:${ExecutionId}:${ExpressId}`	

Chaves de condição do AWS Step Functions

AWS Step Functions define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por um par de chave valor da etiqueta que é permitido na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso por um par de chave e valor da etiqueta de um recurso.	Segmento
aws:TagKeys	Filtra o acesso por uma lista de chaves da etiqueta que são permitidas na solicitação	ArrayOfString
states:HTTPEndpoint	Filtra o acesso pelo endpoint que o estado Tarefa de HTTP permite na solicitação	String
states:HTTPMethod	Filtra o acesso pelo método que o estado Tarefa de HTTP permite na solicitação	String
states:StateMachineQualifier	Filtra o acesso pelo qualificador de um ARN de uma máquina de estado	ArrayOfString

Ações, recursos e chaves de condição do AWS Storage Gateway

AWS O Storage Gateway (prefixo do serviço:`storagegateway`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Storage Gateway

- Tipos de recursos definidos pelo AWS Storage Gateway
- Chaves de condição do AWS Storage Gateway

Ações definidas pelo AWS Storage Gateway

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ActivateGateway	Concede permissão para ativar o gateway que você implantou anteriormente no host	Gravação		aws:RequestTag/${TagKey} aws:TagKeys	
AddCache	Concede permissão para configurar um ou mais discos locais de gateway como cache para um gateway de volume de cache	Gravação	gateway*		
AddTagsToResource	Concede permissão para adicionar uma ou mais etiquetas ao recurso especificado	Marcação	cache-report		
			fs-association		
			gateway		
			share		
			tape		
			tapepool		
			volume		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
AddUploadBuffer	Concede permissão para configurar um ou mais discos locais de gateway como buffer de upload para um gateway especificado	Gravação	gateway*		
AddWorkingStorage	Concede permissão para configurar um ou mais discos locais de gateway como armazenamento funcional para um gateway	Gravação	gateway*		
AssignTapePool	Concede permissão para mover uma fita para o grupo de destino especificado	Gravar	tape*		
			tapepool*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
Associate FileSystem	Concede permissão para associar um sistema de FSx arquivos da Amazon ao gateway de FSx arquivos da Amazon	Gravar	gateway*		ds:DescribeDirectories ec2:DescribeNetworkInterfaces fsx:DescribeFileSystems iam:CreateServiceLinkedRole logs:CreateLogDelivery logs:GetLogDelivery logs:ListLogDeliveries logs:UpdateLogDelivery

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
AttachVolume	Concede permissão para conectar um volume a uma conexão iSCSI e associa o volume ao gateway especificado	Gravação	gateway* volume*		
BypassGovernanceRetention	Concede permissão para que o bloqueio de retenção de governança em um grupo seja ignorado	Gravação	tapepool*		
CancelArchival	Concede permissão para cancelar o arquivamento de uma fita virtual na prateleira de fitas virtuais (VTS), depois que o processo de arquivamento for iniciado.	Gravar	gateway* tape*		
CancelCacheReport	Concede permissão para cancelar um relatório de cache	Gravar	cache-report*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelRetrieval	Concede permissão para cancelar a recuperação de um fita virtual da prateleira de fitas virtuais (VTS) em um gateway, depois que o processo de arquivamento for iniciado	Gravação	gateway*		
			tape*		
CreateCachediSCSIVolume	Concede permissão para criar um volume armazenado em cache em um gateway armazenado em cache especificado Essa operação tem suporte apenas para a arquitetura de volume armazenada em cache no gateway	Gravação	gateway*		
			volume*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNFSFileShare	Concede permissão para criar um compartilhamento de arquivos do NFS em um gateway de arquivos existente	Gravação	gateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSMBFileShare	Concede permissão para criar um compartilhamento de arquivos do SMB em um gateway de arquivos existente	Gravação	gateway*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshot	Concede permissão para iniciar um snapshot de um volume	Gravação	volume*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshotFromVolumeRecoveryPoint	Concede permissão para iniciar um snapshot de um gateway em um ponto de recuperação de volume	Gravação	volume*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStorediSCSIVolume	Concede permissão para criar um volume em um gateway especificado	Gravação	gateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateTapePool	Concede permissão para criar um grupo de fitas	Gravação		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTapeWithBarcode	Concede permissão para criar uma fita virtual usando seu próprio código de barras	Gravação	gateway* tapepool*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTapes	Concede permissão para criar uma ou mais fitas virtuais. Você grava dados em fitas virtuais e, em seguida, arquiva as fitas	Gravação	gateway* tapepool*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAutomaticTapeCreationPolicy	Concede permissão para excluir a política de criação de fita automática configurada em um gateway-VTL	Gravação	gateway*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteBandwidthRateLimit	Concede permissão para excluir os limites da taxa de largura de banda de um gateway	Gravar	gateway*		
DeleteCacheReport	Concede permissão para excluir os metadados associados a um relatório de cache	Gravar	cache-report*		
DeleteChapCredentials	Concede permissão para excluir as credenciais do Challenge-Handshake Authentication Protocol (CHAP) de um destino do iSCSI e de um par de iniciadores especificados.	Gravação	target*		
DeleteFileShare	Concede permissão para excluir um compartilhamento de arquivos de um gateway de arquivos	Gravação	share*		
DeleteGateway	Concede permissão para excluir um gateway	Gravação	gateway*		
DeleteSnapshotSchedule	Concede permissão para excluir um snapshot de um volume	Gravação	volume*		
DeleteTape	Concede permissão para excluir a fita virtual especificada	Gravação	gateway* tape*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteTapeArchive	Concede permissão para excluir a fita virtual especificada da prateleira de fitas virtuais (VTS)	Gravação			
DeleteTapePool	Concede permissão para excluir o grupo de fitas especificado	Gravar	tapepool*		
DeleteVolume	Concede permissão para excluir o volume de gateway especificado que você criou anteriormente usando a CreateStoredi SCSIVolume API CreateCachedi SCSIVolume ou	Gravar	volume*		
DescribeAvailabilityMonitorTest	Concede permissão para obter as informações sobre o teste de monitoramento de alta disponibilidade mais recente que foi realizado no gateway	Leitura	gateway*		
DescribeBandwidthRateLimit	Concede permissão para obter os limites da taxa de largura de banda de um gateway	Leitura	gateway*		
DescribeBandwidthRateLimitSchedule	Concede permissão para obter a programação dos limites da taxa de largura de banda de um gateway	Leitura	gateway*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeCache	Concede permissão para obter informações sobre o cache de um gateway. Essa operação tem suporte apenas para a arquitetura de volume armazenada em cache no gateway	Leitura	gateway*		
DescribeCacheReport	Concede permissão para obter uma descrição de um relatório de cache	Leitura	cache-report*		
DescribeCachediSCSIVolumes	Concede permissão para obter uma descrição dos volumes de gateway especificados na solicitação. Essa operação tem suporte apenas para a arquitetura de volume armazenada em cache no gateway	Leitura	volume*		
DescribeChapCredentials	Concede permissão para obter uma matriz de informações de credenciais do Challenge-Handshake Authentication Protocol (CHAP) para um destino iSCSI especificado, uma para cada par de iniciadores de destino.	Leitura	target*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeFileSystemAssociations	Concede permissão para obter uma descrição de uma ou mais associações de sistemas de arquivos	Leitura	fs-association*		
DescribeGatewayInformation	Concede permissão para obter metadados sobre um gateway, como seu nome, interfaces de rede, fuso horário configurado e o estado (se o gateway está em execução ou não)	Leitura	gateway*		
DescribeMaintenanceStartTime	Concede permissão para obter a hora de início da manutenção semanal do gateway, incluindo a hora e o dia da semana.	Leitura	gateway*		
DescribeNFSFileShares	Concede permissão para obter uma descrição para um ou mais compartilhamentos de arquivos de um gateway de arquivos	Leitura	share*		
DescribeSMBFileShares	Concede permissão para obter uma descrição para um ou mais compartilhamentos de arquivos de um gateway de arquivos	Leitura	share*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeSMBSettings	Concede permissão para obter uma descrição das configurações de compartilhamento de arquivos do Server Message Block (SMB) de um gateway de arquivos.	Leitura	gateway*		
DescribeSnapshotSchedule	Concede permissão para descrever a programação de snapshot para o volume de gateway especificado	Leitura	volume*		
DescribeStorediSCSIVolumes	Concede permissão para obter a descrição dos volumes de gateway especificados na solicitação	Leitura	volume*		
DescribeTapeArchives	Concede permissão para obter uma descrição de fitas virtuais especificadas na prateleira de fitas virtuais (VTS)	Leitura			
DescribeTapeRecoveryPoints	Concede permissão para obter uma lista de pontos de recuperação de fitas virtuais que estão disponíveis para o gateway-VTL especificado.	Leitura	gateway*		
DescribeTapes	Concede permissão para obter uma descrição do Nome de recurso da Amazon (ARN) das fitas virtuais.	Leitura	gateway*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeUploadBuffer	Concede permissão para obter informações sobre o buffer de upload de um gateway	Leitura	gateway*		
DescribeVTLDevices	Concede permissão para obter uma descrição da biblioteca de fitas virtuais (VTL) do gateway especificado	Leitura	gateway*		
DescribeWorkingStorage	Concede permissão para obter informações sobre o armazenamento funcional de um gateway	Leitura	gateway*		
DetachVolume	Concede permissão para desconectar um volume de uma conexão iSCSI e separa o volume do gateway especificado.	Gravação	volume*		
DisableGateway	Concede permissão para desabilitar um gateway quando ele não estiver mais funcionando	Gravar	gateway*		
DisassociateFileSystem	Concede permissão para desassociar um sistema de FSx arquivos da Amazon de um gateway de FSx arquivos da Amazon	Gravar	fs-association*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
EvictFilesFailingUpload	Concede permissão para limpar o cache de um compartilhamento de entradas de arquivo que estão falhando no upload para o Amazon S3	Gravar	share*		
JoinDomain	Concede permissão para que você seja incluído em um domínio do Active Directory	Gravar	gateway*		
ListAutomaticTapeCreationPolicies	Concede permissão para listar as políticas de criação automática de fitas configuradas no gateway-VTL especificado ou em todos os gateways de propriedade de seu VTLs Conta da AWS	Lista			
ListCacheReports	Concede permissão para obter uma lista dos relatórios de cache de propriedade de seu Conta da AWS	Lista			
ListFileShares	Concede permissão para obter uma lista dos compartilhamentos de arquivos de um gateway de arquivos específico ou a lista de compartilhamentos de arquivos pertencentes ao seu Conta da AWS	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListFileSystemAssociations	Concede permissão para obter uma lista das associações do sistema de arquivos para o gateway especificado	Lista			
ListGateways	Concede permissão para listar gateways pertencentes a um Conta da AWS em uma região especificada na solicitação. A lista retornada é solicitada pelo Nome de recurso da Amazon (ARN) do gateway.	Listar			
ListLocalDisks	Concede permissão para obter uma lista dos discos locais do gateway	Listar	gateway*		
ListTagsForResource	Concede permissão para obter as etiquetas que foram adicionadas ao recurso especificado	Lista	gateway		
			share		
			tape		
			volume		
ListTapePools	Concede permissão para listar pools de fitas pertencentes a seu Conta da AWS	Lista			
ListTapes	Concede permissão para listar as fitas virtuais em sua biblioteca de fitas virtuais (VTL) e em sua prateleira de fitas virtuais (VTS).	Listar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListVolumeInitiators	Concede permissão para listar os iniciadores iSCSI que estão conectados a um volume	Listar	volume*		
ListVolumeRecoveryPoints	Concede permissão para listar os pontos de recuperação de um gateway especificado	Listar	gateway*		
ListVolumes	Concede permissão para listar os volumes armazenados iSCSI de um gateway	Lista			
NotifyWhenUploaded	Concede permissão para enviar a você uma notificação por meio de CloudWatch Eventos quando todos os arquivos gravados em seu compartilhamento de arquivos NFS tiverem sido enviados para o Amazon S3	Gravar	share*		
RefreshCache	Concede permissão para atualizar o cache do compartilhamento de arquivos especificado	Gravação	share*		
RemoveTagsFromResource	Concede permissão para remover uma ou mais etiquetas do recurso especificado	Marcação	cache-report		
			fs-association		
			gateway		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			share		
			tape		
			tapepool		
			volume		
				aws:TagKeys	
ResetCache	Concede permissão para redefinir todos os discos de cache que encontraram um erro e disponibiliza os discos para reconfiguração como armazenamento em cache	Gravação	gateway*		
RetrieveTapeArchive	Concede permissão para recuperar uma fita virtual arquivada da prateleira de fita virtual (VTS) para um gateway-VTL	Gravação	gateway*		
			tape*		
RetrieveTapeRecoveryPoint	Concede permissão para recuperar o ponto de recuperação da fita virtual especificada	Gravação	gateway*		
			tape*		
SetLocalConsolePassword	Concede permissão para definir a senha para o console local da VM	Gravação	gateway*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SetSMBGuestPassword	Concede permissão para definir a senha para o usuário convidado do SMB	Gravação	gateway*		
ShutdownGateway	Concede permissão para desligar um gateway	Gravação	gateway*		
StartAvailabilityMonitorTest	Concede permissão para iniciar um teste que verifica se o gateway especificado está configurado para monitoramento de alta disponibilidade no ambiente de host	Gravar	gateway*		
StartCacheReport	Concede permissão para iniciar um relatório de cache para um compartilhamento de arquivos existente	Gravar	share*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartGateway	Concede permissão para iniciar um gateway que você desligou anteriormente	Gravação	gateway*		
UpdateAutomaticTapeCreationPolicy	Concede permissão para atualizar a política de criação automática de fita configurada em um gateway-VTL	Gravação	gateway*		
			tapepool*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateBandwidthRateLimit	Concede permissão para atualizar os limites da taxa de largura de banda de um gateway	Gravação	gateway*		
UpdateBandwidthRateLimitSchedule	Concede permissão para atualizar a programação do limite da taxa de largura de banda de um gateway	Gravação	gateway*		
UpdateChapCredentials	Concede permissão para atualizar as credenciais do Challenge-Handshake Authentication Protocol (CHAP) em um destino do iSCSI especificado	Gravação	target*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateFileSystemAssociation	Concede permissão para atualizar uma associação de sistema de arquivos	Gravação	fs-association*		logs:CreateLogDelivery logs:DeleteLogDelivery logs:GetLogDelivery logs:ListLogDeliveries logs:UpdateLogDelivery
UpdateGatewayInformation	Concede permissão para atualizar os metadados de um gateway, que inclui o nome e o fuso horário do gateway	Gravação	gateway*		
UpdateGatewaySoftwareNow	Concede permissão para atualizar o software da máquina virtual (VM) do gateway	Gravação	gateway*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateMaintenanceStartTime	Concede permissão para atualizar as informações do horário de início da manutenção semanal de um gateway, incluindo a hora e o dia da semana. O horário da manutenção é a hora no fuso horário do gateway.	Gravação	gateway*		
UpdateNFSFileShare	Concede permissão para atualizar um compartilhamento de arquivos do NFS	Gravação	share*		
UpdateSMBFileShare	Concede permissão para atualizar um compartilhamento de arquivos do SMB	Gravação	share*		
UpdateSMBFileShareVisibility	Concede permissão para atualizar se os compartilhamentos em um gateway estão visíveis em uma exibição de rede ou lista de navegação	Gravar	gateway*		
UpdateSMBLocalGroups	Concede permissão para atualizar a lista de usuários e grupos do Active Directory que têm permissões especiais para compartilhamentos de arquivos SMB no gateway	Gravar	gateway*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateSMBSecurityStrategy	Concede permissão para atualizar a estratégia de segurança do SMB em um gateway de arquivos	Gravação	gateway*		
UpdateSnapshotSchedule	Concede permissão para atualizar uma programação de snapshot configurada para um volume de gateway	Gravação	volume*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateVTLDeviceType	Concede permissão para atualizar o tipo de alterador de mídia em um gateway-VTL	Gravar	device*		

Tipos de recursos definidos pelo AWS Storage Gateway

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS Storage Gateway

AWS O Storage Gateway define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelo conjunto de valores permitido para cada uma das etiquetas	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelo valor-etiqueta associado ao recurso	String
aws:TagKeys	Filtra o acesso pela presença de etiquetas obrigatórias na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Supply Chain

AWS A cadeia de suprimentos (prefixo do serviço:`scn`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Supply Chain
- Tipos de recursos definidos pelo AWS Supply Chain

- Chaves de condição para o AWS Supply Chain

Ações definidas pelo AWS Supply Chain

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssignAdminPermissionsToUser	Concede permissão para adicionar permissão AWS de administrador da cadeia de suprimentos ao usuário federado	Gravar	instance*		
CreateBillOfMaterialsImportJob	Concede permissão para criar um BillOfMaterialsImportJob que importará um arquivo CSV de registros BillOfMaterials	Gravar	instance*		
CreateDataIntegrationFlow	Concede permissão para criar DataIntegrationFlow que pode se transformar de várias fontes em um destino	Gravar	instance*		
CreateDataLakeDataset	Concede permissão para criar o conjunto de dados do data lake	Gravar	instance*		
CreateDataLakeNamespace	Concede permissão para criar o namespace do data lake	Gravar	instance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateInstance	Concede permissão para criar uma nova instância da cadeia de AWS suprimentos	Gravar	instance*		
CreateSSOApplication	Concede permissão para criar o aplicativo IAM Identity Center para uma instância da cadeia AWS de suprimentos	Gravar	instance*		
DeleteDataIntegrationFlow	Concede permissão para excluir o DataIntegrationFlow	Gravar	data-integration-flow*		
DeleteDataLakeDataset	Concede permissão para excluir o conjunto de dados do data lake	Gravar	dataset*		
DeleteDataLakeNamespace	Concede permissão para excluir o namespace do data lake	Gravar	namespace*		
DeleteInstance	Concede permissão para excluir uma instância da AWS cadeia de suprimentos	Gravar	instance*		
DeleteSSOApplication	Concede permissão para excluir o aplicativo IAM Identity Center da instância da cadeia AWS de suprimentos	Gravar	instance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeInstance	Concede permissão para visualizar detalhes de uma instância da cadeia de AWS suprimentos	Leitura	instance*		
GetBillOfMaterialsImportJob	Concede permissão para visualizar o status e os detalhes de um BillOfMaterialsImportJob	Leitura	bill-of-materials-import-job*		
GetDataIntegrationEvent	Concede permissão para obter um DataIntegrationEvent	Leitura	instance*		
GetDataIntegrationFlow	Concede permissão para obter os DataIntegrationFlow detalhes	Leitura	data-integration-flow*		
GetDataIntegrationFlowExecution	Concede permissão para obter uma execução específica de uma determinada DataIntegrationFlow	Leitura	data-integration-flow*		
GetDataLakeDataset	Concede permissão para obter os detalhes do conjunto de dados	Leitura	dataset*		
GetDataLakeNamespace	Concede permissão para obter os detalhes do namespace	Leitura	namespace*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetInstance	Concede permissão para visualizar detalhes de uma instância da cadeia de AWS suprimentos	Leitura	instance*		
ListAdminUsers	Concede permissão para listar os administradores da cadeia de AWS suprimentos de uma instância	Lista	instance*		
ListDataIntegrationEvents	Concede permissão para listar tudo DataIntegrationEvents em uma instância	Lista	instance*		
ListDataIntegrationFlowExecutions	Concede permissão para listar todas as execuções de um determinado DataIntegrationFlow	Lista	data-integration-flow*		
ListDataIntegrationFlows	Concede permissão para listar todos os de DataIntegrationFlows forma paginada	Lista	instance*		
ListDataLakeDatasets	Concede permissão para listar os conjuntos de dados do data lake em uma instância e um namespace específicos	Lista	instance*		
ListDataLakeNamespaces	Concede permissão para listar os namespaces do data lake em uma instância específica	Lista	instance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListInstances	Concede permissão para visualizar as instâncias da cadeia de AWS suprimentos associadas a um Conta da AWS	Lista	instance*		
ListTagsForResource	Concede permissão para listar etiquetas para um recurso da cadeia de AWS suprimentos	Lista	instance*		
RemoveAdminPermissionsForUser	Concede permissão para remover a permissão AWS de administrador da cadeia de suprimentos do usuário federado	Gravar	instance*		
SendDataIntegrationEvent	Concede permissão para criar um DataIntegrationEvent que ingerirá dados em tempo real	Gravar	instance*		
TagResource	Concede permissão para marcar um recurso da AWS cadeia de suprimentos	Tags	instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover a tag de um recurso da cadeia de AWS suprimentos	Tags	instance*		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateDataIntegrationFlow	Concede permissão para atualizar o DataIntegrationFlow	Gravar	data-integration-flow*		
UpdateDataLakeDataset	Concede permissão para atualizar o conjunto de dados do data lake	Gravar	dataset*		
UpdateDataLakeNamespace	Concede permissão para atualizar o namespace do data lake	Gravar	namespace*		
UpdateInstance	Concede permissão para atualizar uma instância da AWS cadeia de suprimentos	Gravar	instance*		

Tipos de recursos definidos pelo AWS Supply Chain

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
instance	`arn:${Partition}:scn:${Region}:${Account}:instance/${InstanceId}`	

Tipos de recursos	ARN	Chaves de condição
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}	

Chaves de condição para o AWS Supply Chain

AWS A cadeia de suprimentos define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso usando pares de chave-valor da etiqueta na solicitação	String

Chaves de condição	Descrição	Tipo
aws:ResourceTag/${TagKey}	Filtra o acesso usando pares de chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso usando chaves da etiqueta em uma solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS Support

AWS Support (prefixo do serviço:`support`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Support
- Tipos de recursos definidos pelo AWS Support
- Chaves de condição do AWS Support

Ações definidas pelo AWS Support

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

> **Note**
>
> Suporte fornece a capacidade de acessar, modificar e resolver casos, bem como usar ações do Trusted Advisor. Quando você usa a API de suporte para chamar ações relacionadas ao Trusted Advisor, nenhuma das ações "trustedadvisor:*" restringe seu acesso. As ações “trustedadvisor:*” se aplicam apenas ao Trusted Advisor no AWS Management Console.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddAttachmentsToSet	Concede permissão para adicionar um ou mais anexos a um caso AWS Support	Gravar			
AddCommunicationToCase	Concede permissão para adicionar uma comunicação com o cliente a um AWS Support caso	Gravar			
CreateCase	Concede permissão para criar um novo AWS Support caso	Gravar			
DescribeAttachment	Concede permissão para descrever o detalhe do anexo	Leitura			
DescribeCaseAttributes	Concede permissão para permitir que serviços secundários leiam atributos de AWS Support caso. Essa é uma função gerenciada internamente	Leitura			
DescribeCaseOptions	Concede permissão para descrever as opções disponíveis para um único AWS Support caso. Essa é uma função gerenciada internamente	Leitura			
DescribeCases	Concede permissão para listar AWS Support casos que correspondam às entradas fornecidas	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeCommunication	Concede permissão para obter uma única comunicação e anexos para um único caso AWS Support	Leitura			
DescribeCommunications	Concede permissão para listar as comunicações e os anexos de um ou mais casos AWS Support	Leitura			
DescribeCreateCaseOptions	Concede permissão para descrever as opções disponíveis para criar um caso de suporte	Leitura			
DescribeIssueTypes	Concede permissão para devolver tipos de problemas para AWS Support casos	Leitura			
DescribeServices	Concede permissão para listar AWS serviços e categorias que se aplicam a cada serviço	Leitura			
DescribeSeverityLevels	Concede permissão para listar os níveis de gravidade que podem ser atribuídos a um AWS Support caso	Leitura			
DescribeSupportLevel	Concede permissão para retornar o nível de suporte para um identificador de AWS conta	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeSupportedLanguages	Concede permissão para descrever os idiomas de suporte disponíveis para um determinado código de categoria, código de serviço e tipo de problema	Leitura			
DescribeTrustedAdvisorCheckRefreshStatuses	Concede permissão para obter o status de uma verificação de atualização do Trusted Advisor com base em uma lista de identificadores de verificação	Leitura			
DescribeTrustedAdvisorCheckResult	Concede permissão para obter os resultados da verificação do Trusted Advisor que tem o identificador de verificação especificado	Leitura			
DescribeTrustedAdvisorCheckSummaries	Concede permissão para obter os resumos dos resultados das verificações do Trusted Advisor que têm os identificadores de verificação especificados	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeTrustedAdvisorChecks	Concede permissão para obter uma lista de todas as verificações disponíveis do Trusted Advisor, incluindo nome, identificador, categoria e descrição	Leitura			
GetInteraction	Concede permissão para obter assistência personalizada para solução de problemas técnicos e de conta para uma interação específica	Leitura			
InitiateCallForCase	Concede permissão para iniciar uma chamada no AWS Support Center. Essa é uma função gerenciada internamente	Gravar			
InitiateChatForCase	Concede permissão para iniciar um bate-papo no AWS Support Center.Esta é uma função gerenciada internamente	Gravar			
PutCaseAttributes	Concede permissão para permitir que serviços secundários anexem atributos aos AWS Support casos. Essa é uma função gerenciada internamente	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RateCaseCommunication	Concede permissão para avaliar a comunicação de um AWS Support caso	Gravar			
RefreshTrustedAdvisorCheck	Concede permissão para solicitar uma atualização da verificação do Trusted Advisor que tem o identificador de verificação especificado	Gravar			
ResolveCase	Concede permissão para resolver um AWS Support caso	Gravar			
SearchForCases	Concede permissão para retornar uma lista de AWS Support casos que correspondam às entradas fornecidas	Leitura			
StartInteraction	Concede permissão para iniciar uma interação específica para receber assistência personalizada para solução de problemas técnicos e de conta	Gravar			
UpdateCaseSeverity	Concede permissão para atualizar a gravidade de um único AWS Support caso. Essa é uma função gerenciada internamente	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateInteraction	Concede permissão para atualizar uma interação específica para receber assistência personalizada para solução de problemas técnicos e de conta	Gravar			

Tipos de recursos definidos pelo AWS Support

AWS Support não suporta a especificação de um ARN de recurso no elemento de uma `Resource` declaração de política do IAM. Para conceder acesso ao AWS Support, especifique `"Resource": "*"` na política.

Chaves de condição do AWS Support

O Support não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Support App no Slack

AWS Support O aplicativo no Slack (prefixo do serviço:`supportapp`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Support App no Slack
- Tipos de recursos definidos pelo AWS Support App no Slack
- Chaves de condição para o AWS Support App no Slack

Ações definidas pelo AWS Support App no Slack

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de

recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSlackChannelConfiguration	Concede permissão para criar uma configuração do Chatbot Slack Channel	Gravar			
DeleteAccountAlias	Concede permissão para excluir um domínio da sua conta do .	Gravar			
DeleteSlackChannelConfiguration	Concede permissão para excluir uma configuração do Chatbot Slack Channel	Gravar			
DeleteSlackWorkspaceConfiguration	Concede permissão para excluir uma configuração de espaço de trabalho do Slack na conta	Gravar			
DescribeSlackChannels [somente permissão]	Concede permissão para listar todos os canais públicos do Slack em um workspace que convidaram o aplicativo AWS Support	Leitura			
GetAccountAlias	Concede permissão para criar um alias da sua conta	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSlackOauthParameters [somente permissão]	Concede permissão para obter parâmetros para o OAuth código do Slack, que o AWS Support aplicativo usa para autorizar o espaço de trabalho	Leitura			
ListSlackChannelConfigurations	Concede permissão para listar todos os conjuntos de configuração da sua conta	Leitura			
ListSlackWorkspaceConfigurations	Concede permissão para listar todos os conjuntos de configuração da sua conta	Leitura			
PutAccountAlias	Concede permissão para criar ou atualizar um alias da sua conta	Gravar			
RedeemSlackOauthCode [somente permissão]	Concede permissão para resgatar o OAuth código do Slack, que o AWS Support aplicativo usa para autorizar o espaço de trabalho	Gravar			
RegisterSlackWorkspaceForOrganization	Concede permissão para registrar um espaço de trabalho do Slack para alguém Conta da AWS que faz parte de uma organização	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateSlackChannelConfiguration	Concede permissão para atualizar a configuração de um canal	Gravar			

Tipos de recursos definidos pelo AWS Support App no Slack

AWS Support O aplicativo no Slack não é compatível com a especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para permitir acesso ao AWS Support App no Slack, especifique `"Resource": "*"` na sua política.

Chaves de condição para o AWS Support App no Slack

A Visualização do App Mesh não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do console do AWS Support

AWS Support O console (prefixo do serviço:`support-console`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo console do AWS Support
- Tipos de recurso definidos pelo console do AWS Support

- Chaves de condição do console do AWS Support

Ações definidas pelo console do AWS Support

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CheckSubscription [somente permissão]	Concede permissão para verificar se a conta tem acesso a determinado produto	Leitura			
CreateCaseDraft [somente permissão]	Concede permissão para criar ou atualizar um rascunho de caso para um determinado tipo de caso	Gravar			
CreateContact [somente permissão]	Concede permissão para criar um contato autenticado para um determinado tipo de contato	Gravar			
DeleteCaseDraft [somente permissão]	Concede permissão para excluir um rascunho de caso para um determinado tipo de caso	Gravar			
DescribeDynamicHelp [somente permissão]	Concede permissão para obter recursos de ajuda dinâmicos para determinado serviço e categoria	Leitura			
GetAccountGovCloud	Concede permissão para determinar se a conta de	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
Enabled [somente permissão]	chamada está GovCloud ativada				
GetAccountState [somente permissão]	Concede permissão para obter o estado da conta de chamada	Leitura			
GetBanner [somente permissão]	Concede permissão para obter as informações do banner de suporte	Leitura			
GetCaseDraft [somente permissão]	Concede permissão para obter um rascunho de caso para determinado tipo de caso	Leitura			
GetQuestionnaire [somente permissão]	Concede permissão para receber um questionário de feedback	Leitura			
SaveFeedback [somente permissão]	Concede permissão para salvar o feedback do questionário	Gravar			

Tipos de recurso definidos pelo console do AWS Support

AWS Support O console não suporta a especificação de um ARN de recurso no elemento de uma `Resource` declaração de política do IAM. Para permitir acesso ao console do AWS Support , especifique `"Resource": "*"` na política.

Chaves de condição do console do AWS Support

O Support Console não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Support Plans

AWS Support Os planos (prefixo do serviço:`supportplans`) fornecem os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Support Plans
- Tipos de recursos definidos pelo AWS Support Plans
- Chaves de condição do AWS Support Plans

Ações definidas pelo AWS Support Plans

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSupportPlanSchedule [somente permissão]	Concede permissão para criar cronogramas de planos de suporte para isso Conta da AWS	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSupportPlan [somente permissão]	Concede permissão para visualizar detalhes sobre o plano de suporte atual para isso Conta da AWS	Leitura			
GetSupportPlanUpdateStatus [somente permissão]	Concede permissão para exibir detalhes sobre o status de uma solicitação para atualizar um plano de suporte	Leitura			
ListSupportPlanModifiers [somente permissão]	Concede permissão para visualizar uma lista de todos os modificadores do plano de suporte para isso Conta da AWS	Lista			
StartSupportPlanUpdate [somente permissão]	Concede permissão para atualizar o plano de suporte para isso Conta da AWS	Gravar			

Tipos de recursos definidos pelo AWS Support Plans

AWS Support Os planos não oferecem suporte à especificação de um ARN de recurso no elemento de uma `Resource` declaração de política do IAM. Para permitir acesso ao AWS Support Plans, especifique `"Resource": "*"` na política.

Chaves de condição do AWS Support Plans

O Support Plans não tem chaves de contexto específicas de serviço que podem ser usadas no `Condition` elemento de instruções de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o AWS Sustainability

AWS A sustentabilidade (prefixo do serviço:`sustainability`) fornece os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Sustainability
- Tipos de recursos definidos pelo AWS Sustainability
- Chaves de condição do AWS Sustainability

Ações definidas pelo AWS Sustainability

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetCarbonFootprintSummary	Concede permissão para exibir a ferramenta de pegada de carbono	Leitura			

Tipos de recursos definidos pelo AWS Sustainability

AWS A sustentabilidade não suporta a especificação de um ARN de recurso no elemento de uma `Resource` declaração de política do IAM. Para conceder acesso AWS Sustainability, especifique `"Resource": "*"` na política.

Chaves de condição do AWS Sustainability

O Sustainability não tem chaves de contexto específicas ao serviço que possam ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Systems Manager

AWS O Systems Manager (prefixo do serviço:`ssm`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Systems Manager
- Tipos de recursos definidos pelo AWS Systems Manager
- Chaves de condição do AWS Systems Manager

Ações definidas pelo AWS Systems Manager

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddTagsToResource	Concede permissão para adicionar ou substituir uma ou mais tags para um recurso especificado AWS	Tags	association		
			automation-execution		
			document		
			instance		
			maintenancewindow		
			managed-instance		
			opsitem		
			opsmetadata		
			parameter		
			patchbaseline		
			task		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
AssociateOpsItemRelatedItem	Concede permissão para se RelatedItem associar a um OpsItem	Gravar	opsitem*		
CancelCommand	Concede permissão para cancelar um comando Run Command especificado	Gravação			
CancelMaintenanceWindowExecution	Concede permissão para cancelar uma execução da janela de manutenção em andamento	Gravar	maintenancewindow*		
CreateActivation	Concede permissão para criar uma ativação que é usada para registrar servidores locais e máquinas virtuais (VMs) no Systems Manager	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssociation	Concede permissão para associar um documento especificado do Systems Manager a instâncias especificadas ou outros destinos	Gravar	association*		
			document*		
			instance		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			managed-instance		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssociationBatch	Concede permissão para combinar entradas para várias CreateAssociation operações em um único comando	Gravar	document*		
			instance		
			managed-instance		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateDocument	Concede permissão para criar um documento do Systems Manager SSM	Gravação	document*		iam:PassRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys ssm:DocumentType	
CreateMaintenanceWindow	Concede permissão para criar uma janela de manutenção	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOpsItem	Concede permissão para criar um OpsItem em OpsCenter	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOpsMetadata	Concede permissão para criar um OpsMetadata objeto para um AWS recurso	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreatePatchBaseline	Concede permissão para criar uma linha de base de patch	Gravação		aws:RequestTag/${TagKey} aws:TagKeys	
CreateResourceDataSync	Concede permissão para criar uma configuração de sincronização de dados de recurso, que coleta regularmente dados de inventário de instâncias gerenciadas e atualiza os dados em um bucket do Amazon S3	Gravação	resourcedatasync*		
				ssm:SyncType	
DeleteActivation	Concede permissão para excluir uma ativação especificada para instâncias gerenciadas	Gravação			
DeleteAssociation	Concede permissão para desassociar um documento do SSM especificado de uma instância especificada	Gravação	association		
			document		
			instance		
			managed-instance		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteDocument	Concede permissão para excluir um documento do SSM especificado e suas associações de instância	Gravação	document*		
				ssm:DocumentType	
DeleteInventory	Concede permissão para excluir um tipo de inventário personalizado especificado ou os dados associados a um tipo de inventário personalizado	Gravação			
DeleteMaintenanceWindow	Concede permissão para excluir uma janela de manutenção especificada	Gravar	maintenancewindow*		
DeleteOpsItem	Concede permissão para excluir um OpsItem	Gravar	opsitem*		
DeleteOpsMetadata	Concede permissão para excluir um OpsMetadata objeto	Gravar	opsmetadata*		
DeleteParameter	Concede permissão para excluir um parâmetro do SSM especificado	Gravação	parameter*		
				aws:ResourceTag/${TagKey}	
DeleteParameters	Concede permissão para excluir vários parâmetros do SSM especificados	Gravação	parameter*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
DeletePatchBaseline	Concede permissão para excluir uma linha de base de patch especificada	Gravação	patchbaseline*		
DeleteResourceDataSync	Concede permissão para excluir uma sincronização de dados de recurso especificada	Gravar	resourcedatasync*		
				ssm:SyncType	
DeleteResourcePolicy	Concede permissão para excluir uma política de recursos do Systems Manager	Gerenciamento de permissões	document		
			opsitemgroup		
			parameter		
DeregisterManagedInstance	Concede permissão para cancelar o registro de um servidor on-premises especificado ou uma máquina virtual (VM) do Systems Manager	Gravação	managed-instance*		
				ssm:resourceTag/tag-key	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeregisterPatchBaselineForPatchGroup	Concede permissão para cancelar o registro de uma linha de base de patch especificada de modo a impedir que a linha de base de patch torne-se padrão para um grupo de patches especificado	Gravação	patchbaseline*		
DeregisterTargetFromMaintenanceWindow	Concede permissão para cancelar o registro de um destino especificado de uma janela de manutenção	Gravação	maintenancewindow*		
			windowtarget*		
DeregisterTaskFromMaintenanceWindow	Concede permissão para cancelar o registro de uma tarefa especificada de uma janela de manutenção	Gravação	maintenancewindow*		
			windowtask*		
DescribeActivations	Concede permissão para exibir detalhes sobre uma ativação de instância gerenciada especificada, como quando ela foi criada e o número de instâncias registradas usando a ativação	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeAssociation	Concede permissão para exibir detalhes sobre a associação especificada para uma instância ou destino especificado	Leitura	association		
			document		
			instance		
			managed-instance		
				aws:ResourceTag/${TagKey}	
DescribeAssociationExecutionTargets	Concede permissão para exibir informações sobre uma execução de associação especificada	Leitura	association*		
				aws:ResourceTag/${TagKey}	
DescribeAssociationExecutions	Concede permissão para exibir todas as execuções de uma associação especificada	Leitura	association*		
				aws:ResourceTag/${TagKey}	
DescribeAutomationExecutions	Concede permissão para exibir detalhes sobre todas as execuções de automação ativas e encerradas	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeAutomationStepExecutions	Concede permissão para exibir informações sobre todas as execuções de etapas ativas e finalizadas em um fluxo de trabalho de automação	Leitura	automation-execution*		
DescribeAvailablePatches	Concede permissão para exibir todos os patches elegíveis para inclusão em uma linha de base de patch	Leitura			
DescribeDocument	Concede permissão para exibir detalhes sobre um documento do SSM especificado	Leitura	document*		
				ssm:DocumentType	
DescribeDocumentParameters	Concede permissão para exibir informações sobre parâmetros de documento do SSM no console do Systems Manager (ação interna do Systems Manager)	Leitura	document*		
DescribeDocumentPermission	Concede permissão para exibir as permissões de um documento do SSM especificado	Leitura	document*		
				ssm:DocumentType	
DescribeEffectiveInstanceAssociations	Concede permissão para exibir todas as associações atuais de uma instância especificada	Leitura	instance*		
			managed-instance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
DescribeEffectivePatchesForPatchBaseline	Concede permissão para exibir detalhes sobre os patches atualmente associados à linha de base de patch especificada (somente Windows)	Leitura	patchbaseline*		
DescribeInstanceAssociationsStatus	Concede permissão para exibir o status das associações de uma instância especificada	Leitura	instance*		
			managed-instance*		
				aws:ResourceTag/${TagKey}	
DescribeInstanceInformation	Concede permissão para exibir detalhes sobre uma instância especificada	Leitura			
DescribeInstancePatchStates	Concede permissão para exibir detalhes de status sobre patches em uma instância especificada	Leitura	instance*		
			managed-instance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}	
DescribeInstancePatchStatesForPatchGroup	Concede permissão para descrever o estado do patch de alto nível das instâncias no grupo de patches especificado	Leitura			
DescribeInstancePatches	Concede permissão para exibir detalhes gerais sobre os patches em uma instância especificada	Leitura	instance*		
			managed-instance*		
				aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}	
DescribeInstanceProperties	Concede permissão ao EC2 console Amazon do usuário para renderizar os nós das instâncias gerenciadas	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeInventoryDeletions	Concede permissão para exibir detalhes sobre uma exclusão de inventário especificada	Leitura			
DescribeMaintenanceWindowExecutionTaskInvocations	Concede permissão para exibir detalhes de uma execução de tarefa especificada para uma janela de manutenção	Listar			
DescribeMaintenanceWindowExecutionTasks	Concede permissão para exibir detalhes sobre as tarefas realizadas durante a execução de uma janela de manutenção especificada	Listar			
DescribeMaintenanceWindowExecutions	Concede permissão para exibir as execuções de uma janela de manutenção especificada	Listar	maintenancewindow*		
DescribeMaintenanceWindowSchedule	Concede permissão para exibir detalhes sobre execuções futuras de uma janela de manutenção especificada	Listar			
DescribeMaintenanceWindowTargets	Concede permissão para exibir uma lista dos destinos associados a uma janela de manutenção especificada	Listar	maintenancewindow*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeMaintenanceWindowTasks	Concede permissão para exibir uma lista das tarefas associadas a uma janela de manutenção especificada	Listar	maintenancewindow*		
DescribeMaintenanceWindows	Concede permissão para exibir informações sobre todas as janelas de manutenção ou sobre as janelas de manutenção especificadas	Listar			
DescribeMaintenanceWindowsForTarget	Concede permissão para exibir informações sobre os destinos da janela de manutenção e as tarefas associadas a uma instância especificada	Lista			
DescribeOpsItems	Concede permissão para visualizar detalhes sobre especificados OpsItems	Leitura			
DescribeParameters	Concede permissão para exibir detalhes sobre um parâmetro do SSM especificado	Listar			
DescribePatchBaselines	Concede permissão para exibir informações sobre linhas de base de patch que atendem aos critérios especificados	Listar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribePatchGroupState	Concede permissão para exibir detalhes de status agregados para patches de um grupo de patches especificado	Lista			
DescribePatchGroups	Concede permissão para exibir informações sobre a lista de referência de patches para um grupo de patches especificado	Listar			
DescribePatchProperties	Concede permissão para exibir detalhes de patches disponíveis para um sistema operacional especificado e uma propriedade de patch	Listar			
DescribeSessions	Concede permissão para exibir uma lista de sessões recentes do gerenciador de sessão que atendem aos critérios de pesquisa especificados	Lista			
DisassociateOpsItemRelatedItem	Concede permissão para se desassociar RelatedItem de um OpsItem	Gravar	opsitem*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ExecuteAPI	Concede permissão a um administrador delegado do Systems Manager para visualizar detalhes de recursos relacionados OpsItems em várias AWS contas no AWS Management Console	Leitura			
GetAccessToken	Concede permissão para retornar um conjunto de credenciais para ser usado com acesso ao just-in-time nó	Leitura	opsitem*		
GetAutomationExecution	Concede permissão para exibir detalhes de uma execução de automação especificada	Leitura	automation-execution*		
				aws:ResourceTag/${TagKey}	
GetCalendar [somente permissão]	Concede permissão para visualizar detalhes de um calendário específico	Leitura	document*		
GetCalendarState	Concede permissão para visualizar o estado do calendário de um calendário de alteração ou de uma lista de calendários de alteração	Leitura	document*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetCommandInvocation	Concede permissão para exibir detalhes sobre a execução do comando de uma invocação ou plugin especificado	Leitura			
GetConnectionStatus	Concede permissão para exibir o status de conexão do gerenciador de sessão para uma instância gerenciada especificada	Leitura	instance		
			managed-instance		
			task		
				ssm:resourceTag/${TagKey} aws:ResourceTag/${TagKey}	
GetDefaultPatchBaseline	Concede permissão para exibir a lista de referência de patches padrão atual para um tipo de sistema operacional especificado	Leitura	patchbaseline*		
GetDeployablePatchSnapshotForInstance	Concede permissão para recuperar o snapshot da lista de referência de patches atual para uma instância especificada	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetDocument	Concede permissão para visualizar o conteúdo de um documento do SSM especificado	Leitura	document*		
				ssm:DocumentCategories ssm:DocumentType	
GetExecutionPreview	Concede permissão para recuperar uma visualização existente que mostra os efeitos que a execução de um runbook de automação específico teria nos recursos de destino	Leitura			
GetInventory	Concede permissão para exibir detalhes do inventário da instância de acordo com os critérios especificados	Leitura			
GetInventorySchema	Concede permissão para exibir uma lista de tipos de inventário ou nomes de atributos para um tipo de item de inventário especificado	Leitura			
GetMaintenanceWindow	Concede permissão para exibir detalhes sobre uma janela de manutenção especificada	Leitura	maintenancewindow*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetMaintenanceWindowExecution	Concede permissão para exibir detalhes sobre a execução de uma janela de manutenção especificada	Leitura			
GetMaintenanceWindowExecutionTask	Concede permissão para exibir detalhes sobre a tarefa de execução de uma janela de manutenção especificada	Leitura			
GetMaintenanceWindowExecutionTaskInvocation	Concede permissão para exibir detalhes sobre a tarefa de uma janela de manutenção específica em execução em um destino específico	Leitura			
GetMaintenanceWindowTask	Concede permissão para exibir detalhes sobre tarefas registradas com uma janela de manutenção especificada	Leitura	maintenancewindow*		
GetManifest [somente permissão]	Concede permissão ao Systems Manager e ao SSM Agent para determinar os requisitos de instalação do pacote para uma instância (chamada interna do Systems Manager)	Leitura			
GetOpsItem	Concede permissão para visualizar informações sobre um determinado OpsItem	Leitura	opsitem*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetOpsMetadata	Concede permissão para recuperar um objeto OpsMetadata	Leitura	opsmetadata*		
GetOpsSummary	Concede permissão para visualizar informações resumidas com OpsItems base em filtros e agregadores especificados	Leitura	resourcedatasync*		
GetParameter	Concede permissão para exibir informações sobre um parâmetro especificado	Leitura	parameter*		
				aws:ResourceTag/${TagKey}	
GetParameterHistory	Concede permissão para exibir detalhes e alterações para um parâmetro especificado	Leitura	parameter*		
				aws:ResourceTag/${TagKey}	
GetParameters	Concede permissão para exibir informações sobre vários parâmetros especificados	Leitura	parameter*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetParametersByPath	Concede permissão para exibir informações sobre parâmetros em uma hierarquia especificada	Leitura	parameter*		
				ssm:Recursive	
GetPatchBaseline	Concede permissão para exibir informações sobre uma lista de referência de patches especificada	Leitura	patchbaseline*		
GetPatchBaselineForPatchGroup	Concede permissão para exibir o ID da lista de referência de patches atual para um grupo de patches especificado	Leitura			
GetResourcePolicies	Concede permissão para recuperar listas de políticas de recursos do Systems Manager	Lista	document		
			opsitemgroup		
			parameter		
GetServiceSetting	Concede permissão para visualizar a configuração no nível da conta de um serviço AWS	Leitura	servicesetting*		
LabelParameterVersion	Concede permissão para aplicar um rótulo de identificação a uma versão especificada de um parâmetro	Gravação	parameter*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAssociationVersions	Concede permissão para listar versões da associação especificada	List	association*		
				aws:ResourceTag/${TagKey}	
ListAssociations	Concede permissão para listar as associações de um documento do SSM especificado ou uma instância gerenciada	Listar			
ListCommandInvocations	Concede permissão para listar informações sobre invocações de comando enviadas para uma instância especificada	Lista			
ListCommands	Concede permissão para listar os comandos enviados para uma instância especificada	Lista			
ListComplianceItems	Concede permissão para listar status de conformidade para os tipos de recursos especificados em um recurso especificado	Listar			
ListComplianceSummaries	Concede permissão para listar uma contagem de resumo de recursos compatíveis e não compatíveis para um tipo de conformidade especificada	Listar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDocumentMetadataHistory	Concede permissão para exibir o histórico de metadados sobre um documento SSM especificado	Lista	document*		
				ssm:DocumentType	
ListDocumentVersions	Concede permissão para listar todas as versões de um documento especificado	Listar	document*		
				ssm:DocumentType	
ListDocuments	Concede permissão para exibir informações sobre um documento do SSM especificado	Lista			
ListInstanceAssociations	Concede permissão ao SSM Agent para verificar se há novas associações do gerenciador de estados (chamada interna do Systems Manager)	Lista	instance		
			managed-instance		
				aws:ResourceTag/${TagKey}	
ListInventoryEntries	Concede permissão para exibir uma lista de tipos de inventário especificados para uma instância especificada	Lista			
ListNodes	Concede permissão para visualizar detalhes sobre nós gerenciados com base em filtros especificados	Lista	resourcedatasync*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListNodesSummary	Concede permissão para visualizar informações resumidas sobre nós gerenciados com base em filtros e agregadores especificados	Lista	resourcedatasync*		
ListOpsItemEvents	Concede permissão para visualizar detalhes sobre OpsItemEvents	Lista			
ListOpsItemRelatedItems	Concede permissão para visualizar detalhes sobre OpsItem RelatedItems	Lista			
ListOpsMetadata	Concede permissão para visualizar uma lista de OpsMetadata objetos	Lista			
ListResourceComplianceSummaries	Concede permissão para listar a contagem resumida no nível de recursos	Listar			
ListResourceDataSync	Concede permissão para listar informações sobre configurações de sincronização de dados de recursos em uma conta	Listar		ssm:SyncType	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTagsForResource	Concede permissão para visualizar uma lista de etiquetas de recursos para um recurso especificado	Lista	association		
			automation-execution		
			document		
			maintenancewindow		
			managed-instance		
			opsitem		
			opsmetadata		
			parameter		
			patchbaseline		
				aws:ResourceTag/${TagKey}	
ModifyDocumentPermission	Concede permissão para compartilhar um documento SSM personalizado de forma pública ou privada com contas específicas AWS	Gerenciamento de permissões	document*		
				ssm:DocumentType	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutCalendar [somente permissão]	Concede permissão para create/edit um calendário específico	Gravar	document*		
PutComplianceItems	Concede permissão para registrar um tipo de conformidade e outros detalhes de conformidade em um recurso designado.	Gravar	instance		
			managed-instance		
				ssm:SourceInstanceARN ec2:SourceInstanceARN	
PutConfigurePackageResult [somente permissão]	Concede permissão ao SSM Agent para gerar um relatório dos resultados de solicitações específicas do agente (chamada interna do Systems Manager)	Leitura			
PutInventory	Concede permissão para adicionar ou atualizar itens de inventário em várias instâncias gerenciadas especificadas	Gravação		ssm:InventoryTypeName	
PutParameter	Concede permissão para criar um parâmetro do SSM	Gravar	parameter*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys ssm:Overwrite ssm:Policies	
PutResourcePolicy	Concede permissão para criar ou atualizar uma política de recurso do Systems Manager	Gerenciamento de permissões	document		
			opsitemgroup		
			parameter		
RegisterDefaultPatchBaseline	Concede permissão para especificar a lista de referência de patches padrão para um tipo de sistema operacional	Gravar	patchbaseline*		
RegisterManagedInstance	Concede permissão para registrar um Systems Manager Agent	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RegisterPatchBaselineForPatchGroup	Concede permissão para especificar a linha de base de patch padrão para um grupo de patches especificado	Gravação	patchbaseline*		
RegisterTargetWithMaintenanceWindow	Concede permissão para registrar um destino com uma janela de manutenção especificada	Gravação	maintenancewindow*		
RegisterTaskWithMaintenanceWindow	Concede permissão para registrar uma tarefa com uma janela de manutenção especificada	Gravação	maintenancewindow*		
RemoveTagsFromResource	Concede permissão para remover uma chave da etiqueta especificada de um recurso especificado	Tags	association		
			automation-execution		
			document		
			instance		
			maintenancewindow		
			managed-instance		
			opsitem		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			opsmetadata		
			parameter		
			patchbaseline		
			task		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ResetServiceSetting	Concede permissão para redefinir a configuração do serviço de an Conta da AWS para o valor padrão	Gravar	servicesetting*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ResumeSession	Concede permissão para reconectar uma sessão do gerenciador de sessão a uma instância gerenciada	Gravação	session*		
				ssm:resourceTag/aws:ssmmessages:session-id ssm:resourceTag/aws:ssmmessages:target-id	
SendAutomationSignal	Concede permissão para enviar um sinal para alterar o comportamento ou status atual da execução de uma automação especificada	Gravação	automation-execution*		
				aws:ResourceTag/${TagKey}	
SendCommand	Concede permissão para executar comandos em uma ou mais instâncias gerenciadas especificadas	Gravar	document*		
			bucket		
			instance		
			managed-instance		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}	
StartAccessRequest	Concede permissão para iniciar o fluxo de trabalho para sessões de acesso ao just-in-time nó	Gravar	instance		
			managed-instance		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartAssociationsOnce	Concede permissão para executar manualmente uma associação especificada	Gravação	association*		
				aws:ResourceTag/${TagKey}	
StartAutomationExecution	Concede permissão para iniciar a execução de um Documento de automação	Gravação	automation-definition*		
			document*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
StartChangeRequestExecution	Concede permissão para iniciar a execução de um documento Modelo de Alteração de Automação	Gravar	automation-definition*		
			document*		
				aws:RequestTag/${TagKey} aws:TagKeys ssm:AutoApprove	
StartExecutionPreview	Concede permissão para criar uma pré-visualização mostrando os efeitos que a execução de um runbook de automação específico teria nos recursos de destino	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartSession	Concede permissão para iniciar uma conexão com um destino especificado para uma sessão do gerenciador de sessão	Gravação	document		
			instance		
			managed-instance		
			task		
				ssm:SessionDocumentAccessCheck ssm:resourceTag/${TagKey} aws:ResourceTag/${TagKey} ssm:AccessRequestId	
StopAutomationExecution	Concede permissão para interromper uma execução de automação especificada que já está em andamento	Gravação	automation-execution*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TerminateSession	Concede permissão para encerrar permanentemente uma conexão do Gerenciador de Sessões a uma instância	Gravar	session*		
				ssm:resourceTag/aws:ssmmessages:session-id ssm:resourceTag/aws:ssmmessages:target-id	
UnlabelParameterVersion	Concede permissão para remover um rótulo de identificação de uma versão especificada de um parâmetro	Gravar	parameter*		
				aws:ResourceTag/${TagKey}	
UpdateAssociation	Concede permissão para atualizar uma associação e executar imediatamente a associação nos destinos especificados	Gravação	association*		
			document		
			instance		
			managed-instance		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
UpdateAssociationStatus	Concede permissão para atualizar o status do documento do SSM associado a uma instância especificada	Gravação	document*		
			instance		
			managed-instance		
				ssm:SourceInstanceARN ec2:SourceInstanceARN aws:ResourceTag/${TagKey}	
UpdateDocument	Concede permissão para atualizar um ou mais valores para um documento do SSM	Gravação	document*		
				ssm:DocumentType	
UpdateDocumentDefaultVersion	Concede permissão para alterar a versão padrão de um documento do SSM	Gravação	document*		
				ssm:DocumentType	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateDocumentMetadata	Concede permissão para atualizar os metadados de um documento SSM	Gravar	document*		
				ssm:DocumentType	
UpdateInstanceAssociationStatus [somente permissão]	Concede permissão ao SSM Agent para atualizar o status da associação que está sendo executada no momento (chamada interna do Systems Manager)	Gravar	association*		
			instance		
			managed-instance		
				ssm:SourceInstanceARN ec2:SourceInstanceARN aws:ResourceTag/${TagKey}	
UpdateInstanceInformation	Concede permissão ao SSM Agent para enviar um sinal de pulsação para o serviço Systems Manager na nuvem	Gravar	instance		
			managed-instance		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				ssm:SourceInstanceARN ec2:SourceInstanceARN	
UpdateMaintenanceWindow	Concede permissão para atualizar uma janela de manutenção especificada	Gravação	maintenancewindow*		
UpdateMaintenanceWindowTarget	Concede permissão para atualizar um destino da janela de manutenção especificada	Gravação	maintenancewindow*		
			windowtarget*		
UpdateMaintenanceWindowTask	Concede permissão para atualizar uma tarefa de janela de manutenção especificada	Gravação	maintenancewindow*		
			windowtask*		
UpdateManagedInstanceRole	Concede permissão para atribuir ou alterar a função do IAM atribuída a uma instância gerenciada especificada	Gravar	iam-role*		
			managed-instance*		
				ssm:resourceTag/tag-key	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateOpsItem	Concede permissão para editar ou alterar um OpsItem	Gravar	opsitem*		
UpdateOpsMetadata	Concede permissão para atualizar um OpsMetadata objeto	Gravação	opsmetadata*		
UpdatePatchBaseline	Concede permissão para atualizar uma linha de base de patch especificada	Gravação	patchbaseline*		
UpdateResourceDataSync	Concede permissão para atualizar uma sincronização de dados de recursos	Gravar	resourcedatasync*		
				ssm:SyncType	
UpdateServiceSetting	Concede permissão para atualizar a configuração do serviço para um Conta da AWS	Gravar	servicesetting*		

Tipos de recursos definidos pelo AWS Systems Manager

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

> **Note**
>
> Alguns parâmetros da API do State Manager foram defasados. Isso pode causar um comportamento inesperado. Para obter mais informações, consulte Trabalhar com associações usando o IAM.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
task	`arn:${Partition}:ecs:${Region}:${Account}:task/${TaskId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Systems Manager

AWS O Systems Manager define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas solicitações "Criar" com base no conjunto de valores permitidos para uma etiqueta especificada	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso com base em um par de chave-valor de tag atribuído ao recurso AWS	String
aws:TagKeys	Filtra o acesso pelas solicitações "Criar" com base em na inclusão das etiquetas obrigatórias na solicitação	ArrayOfString
ec2:SourceInstanceARN	Filtra o acesso pelo ARN da instância da qual a solicitação se originou.	ARN
ssm:AccessRequestId	Filtra o acesso verificando se um usuário tem acesso à ID da solicitação de acesso especificada na solicitação	String
ssm:AutoApprove	Filtra o acesso verificando se o usuário tem permissão para iniciar fluxos de trabalho do Change Manager sem	Bool

Chaves de condição	Descrição	Tipo
	uma etapa de revisão (com exceção dos eventos de congelamento de alterações)	
ssm:DocumentCategories	Filtra o acesso verificando se o usuário tem permissão para acessar um documento pertencente a uma categoria enum específica	ArrayOfString
ssm:DocumentType	Filtra o acesso verificando se um usuário tem permissão para acessar um documento pertencente a um tipo de documento específico. Disponível somente nas partições “aws”, “aws-cn” e "aws-us-gov”	String
ssm:InventoryTypeName	Filtra o acesso verificando se um usuário também tem acesso ao InventoryType especificado na solicitação	ArrayOfString
ssm:Overwrite	Filtra o acesso controlando se os parâmetros do Systems Manager podem ser substituídos	String
ssm:Policies	Filtra o acesso controlando se uma entidade do IAM (usuário ou perfil) pode criar ou atualizar um parâmetro que inclua uma política de parâmetros	String
ssm:Recursive	Filtra o acesso pelos parâmetros do Systems Manager criados em uma estrutura hierárquica	String
ssm:SessionDocumentAccessCheck	Filtra o acesso verificando se um usuário tem permissão para acessar o documento de configuração padrão do Gerenciador de Sessões ou o documento de configuração personalizado especificado em uma solicitação	Bool
ssm:SourceInstanceARN	Filtra o acesso verificando o Amazon Resource Name (ARN) da instância gerenciada AWS do Systems Manager a partir da qual a solicitação é feita. Essa chave não está presente quando a solicitação vem da instância gerenciada autenticada com uma função do IAM associada ao perfil da EC2 instância.	ARN

Chaves de condição	Descrição	Tipo
ssm:SyncType	Filtra o acesso verificando se um usuário também tem acesso ao ResourceDataSync SyncType especificado na solicitação	String
ssm:resourceTag/${TagKey}	Filtra o acesso por um par de chave/valor da etiqueta atribuído ao recurso Systems Manager	String
ssm:resourceTag/aws:ssmmessages:session-id	Filtra o acesso com base em um par de chave-valor de tag atribuído ao recurso de sessão do Systems Manager	String
ssm:resourceTag/aws:ssmmessages:target-id	Filtra o acesso com base em um par de chave-valor de tag atribuído ao recurso de sessão do Systems Manager	String
ssm:resourceTag/tag-key	Filtra o acesso com base em um par de chave-valor da etiqueta atribuído ao recurso Systems Manager	String

Ações, recursos e chaves de condição do AWS Systems Manager para SAP

AWS O Systems Manager for SAP (prefixo do serviço:`ssm-sap`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Systems Manager para SAP
- Tipos de recursos definidos pelo AWS Systems Manager para SAP
- Chaves de condição do AWS Systems Manager para SAP

Ações definidas pelo AWS Systems Manager para SAP

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BackupDatabase	Concede permissão para executar operação de backup em uma base de dados especificada	Gravar			
DeleteResourcePermission	Concede permissão para excluir as permissões de recursos de nível do SSM para SAP associadas a um recurso de banco de dados SSM para SAP	Gravar			
DeregisterApplication	Concede permissão para cancelar o registro de uma aplicação de SAP com o SSM para SAP	Gravar	application		
GetApplication	Concede permissão para acessar informações sobre uma aplicação registrada no SSM para SAP fornecendo o	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	ID da aplicação ou o ARN da aplicação				
GetComponent	Concede permissão para acessar informações sobre um componente registrado no SSM para SAP fornecendo o ID da aplicação e o ID do componente	Leitura	component		
GetDatabase	Concede permissão para acessar informações sobre um banco de dados registrado no SSM para SAP fornecendo o ID da aplicação, o ID do componente e o ID do banco de dados	Leitura			
GetOperation	Concede permissão para acessar informações sobre uma operação fornecendo seu ID de operação	Leitura			
GetResourcePermission	Concede permissão para obter as permissões de recursos de nível do SSM para SAP associadas a um recurso de banco de dados SSM para SAP	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListApplications	Concede permissão para recuperar uma lista de todos os aplicativos registrados no SSM for SAP do cliente Conta da AWS	Lista			
ListComponents	Concede permissão para recuperar uma lista de todos os componentes na conta do cliente ou de uma aplicação específica	Lista	application		
ListDatabases	Concede permissão para recuperar uma lista de todos os bancos de dados na conta do cliente ou de uma aplicação específica	Lista			
ListOperationEvents	Concede permissão para recuperar uma lista de todos os eventos de operação em uma operação especificada	Lista			
ListOperations	Concede permissão para recuperar uma lista de todas as operações na conta do cliente, podendo ser aplicados filtros adicionais	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas em um ARN de recurso especificado	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutResourcePermission	Concede permissão para adicionar as permissões de recursos de nível do SSM para SAP associadas a um recurso de banco de dados SSM para SAP	Gravar			
RegisterApplication	Concede permissão para registrar uma aplicação de SAP com o SSM para SAP	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
RestoreDatabase	Concede permissão para restaurar um banco de dados a partir de outro banco de dados	Gravar			
StartApplication	Concede permissão para iniciar uma aplicação registrada do SSM para SAP	Gravar	application		
StartApplicationRefresh	Concede permissão para iniciar uma descoberta sob demanda de um aplicativo SSM registrado para SAP	Gravar	application		
StopApplication	Concede permissão para interromper uma aplicação registrada do SSM para SAP	Gravar	application		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para marcar um ARN de recurso especificado	Tags	application		
			component		
			database		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover etiquetas de UM ARN de recurso especificado	Tags	application		
			component		
			database		
				aws:TagKeys	
UpdateApplicationSettings	Concede permissão para atualizar configurações de uma aplicação de SSM para SAP registrada	Gravar	application		
UpdateHANABackupSettings	Concede permissão para atualizar configurações de backup do HANA de um banco de dados especificado	Gravar			

Tipos de recursos definidos pelo AWS Systems Manager para SAP

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS Systems Manager para SAP

AWS O Systems Manager for SAP define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Systems Manager GUI Connect

AWS O Systems Manager GUI Connect (prefixo do serviço:`ssm-guiconnect`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Systems Manager GUI Connect
- Tipos de recursos definidos pelo AWS Systems Manager GUI Connect
- Chaves de condição do AWS Systems Manager GUI Connect

Ações definidas pelo AWS Systems Manager GUI Connect

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando

usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelConnection [somente permissão]	Concede permissão para encerrar uma conexão do GUI Connect	Gravar			
DeleteConnectionRecordingPreferences	Concede permissão para remover as preferências de gravação da conexão GUI Connect	Gravar			
GetConnection [somente permissão]	Concede permissão para obter os metadados de uma conexão do GUI Connect	Leitura			
GetConnectionRecordingPreferences	Concede permissão para obter as preferências de gravação da conexão GUI Connect	Leitura			
ListConnections [somente permissão]	Concede permissão para listar os metadados para conexões do GUI Connect	Lista			
StartConnection [somente permissão]	Concede permissão para iniciar uma conexão do GUI Connect	Gravar			
UpdateConnectionRecordingPreferences	Concede permissão para atualizar as preferências de gravação da conexão GUI Connect	Gravar			

Tipos de recursos definidos pelo AWS Systems Manager GUI Connect

AWS O Systems Manager GUI Connect não suporta a especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para permitir ao acesso ao AWS Systems Manager GUI Connect, especifique `"Resource": "*"` Em sua política.

Chaves de condição do AWS Systems Manager GUI Connect

O GUI Connect não tem chaves de contexto específicas ao serviço que possam ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Systems Manager Incident Manager

AWS O Systems Manager Incident Manager (prefixo do serviço:`ssm-incidents`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Systems Manager Incident Manager
- Tipos de recursos definidos pelo AWS Systems Manager Incident Manager
- Chaves de condição do AWS Systems Manager Incident Manager

Ações definidas pelo AWS Systems Manager Incident Manager

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchGetIncidentFindings	Concede permissão para recuperar detalhes sobre descobertas especificadas para um registro de incidente	Leitura	incident-record*		
			response-plan*		
CreateReplicationSet	Concede permissão para criar um grupo de replicações.	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole ssm-incidents:TagResource
CreateResponsePlan	Concede permissão para criar um plano de resposta.	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:PassRole ssm-incidents:TagResource
CreateTimelineEvent	Concede permissão para criar um evento do cronograma de um registro de incidente.	Write	incident-record*		
			response-plan*		
DeleteIncidentRecord	Concede permissão para excluir um registro de incidente.	Write	incident-record*		
DeleteReplicationSet	Concede permissão para excluir um grupo de replicações.	Write	replication-set*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteResourcePolicy	Concede permissão para excluir a política de recursos de um plano de resposta.	Permissions management	response-plan*		
DeleteResponsePlan	Concede permissão para excluir um plano de resposta.	Write	response-plan*		
DeleteTimelineEvent	Concede permissão para excluir um evento do cronograma.	Write	incident-record*		
GetIncidentRecord	Concede permissão para visualizar o conteúdo de um registro de incidente.	Read	incident-record*		
			response-plan*		
GetReplicationSet	Concede permissão para visualizar o grupo de replicações.	Read	replication-set*		
GetResourcePolicies	Concede permissão para visualizar as políticas de recursos de um plano de resposta.	Read	response-plan*		
GetResponsePlan	Concede permissão para visualizar o conteúdo de um plano de resposta especificado.	Read	response-plan*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetTimelineEvent	Concede permissão para visualizar um evento do cronograma.	Leitura	incident-record*		
			response-plan*		
ListIncidentFindings	Concede permissão para listar descobertas para um registro de incidente	Lista	incident-record*		
			response-plan*		
ListIncidentRecords	Concede permissão para listar o conteúdo de todos os registros de incidente.	Lista			
ListRelatedItems	Concede permissão para listar os itens relacionados a um registro de incidente	Lista	incident-record*		
			response-plan*		
ListReplicationSets	Concede permissão para listar todos os conjuntos de replicações.	List			
ListResponsePlans	Concede permissão para listar todos os planos de resposta.	List			
ListTagsForResource	Concede permissão para visualizar uma lista de etiquetas de recursos para um recurso especificado	Read	incident-record		
			replication-set		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			response-plan		
ListTimelineEvents	Concede permissão para listar todos os eventos do cronograma de um registro de incidente.	List	incident-record*		
			response-plan*		
PutResourcePolicy	Concede permissão para adicionar a política de recursos a um plano de resposta.	Permissions management	response-plan*		
StartIncident	Concede permissão para iniciar um novo incidente usando um plano de resposta	Write	response-plan*		
TagResource	Concede permissão para adicionar etiquetas a um plano de resposta.	Marcação	incident-record		
			replication-set		
			response-plan		
				aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para remover etiquetas de um plano de resposta.	Marcação	incident-record		
			replication-set		
			response-plan		
				aws:TagKeys	
UpdateDeletionProtection	Concede permissão para atualizar a proteção contra a exclusão de grupos de replicações.	Write	replication-set*		
UpdateIncidentRecord	Concede permissão para atualizar o conteúdo de um registro de incidente.	Write	incident-record*		
			response-plan*		
UpdateRelatedItems	Concede permissão para atualizar os itens relacionados a um registro de incidente.	Write	incident-record*		
			response-plan*		
UpdateReplicationSet	Concede permissão para atualizar um grupo de replicações.	Write	replication-set*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateResponsePlan	Concede permissão para atualizar o conteúdo de um plano de resposta.	Write	response-plan*		iam:PassRole ssm-incidents:TagResource
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateTimelineEvent	Concede permissão para atualizar um evento do cronograma.	Write	incident-record*		
			response-plan*		

Tipos de recursos definidos pelo AWS Systems Manager Incident Manager

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS Systems Manager Incident Manager

AWS O Systems Manager Incident Manager define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Systems Manager Incident Manager Contacts

AWS Os contatos do Systems Manager Incident Manager (prefixo do serviço:`ssm-contacts`) fornecem os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Systems Manager Incident Manager Contacts
- Tipos de recurso definidos pelo AWS Systems Manager Incident Manager Contacts
- Chaves de condição do AWS Systems Manager Incident Manager Contacts

Ações definidas pelo AWS Systems Manager Incident Manager Contacts

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar

a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptPage	Concede permissão para aceitar uma página.	Write	page*		
ActivateContactChannel	Concede permissão para ativar o canal de comunicação de um contato.	Write	contactchannel*		
AssociateContact [somente permissão]	Concede permissão para usar um contato em um plano de escalonamento.	Permissions management	contact*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateContact	Concede permissão para criar um contato	Write	contact*		ssm-contacts:AssociateContact
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateContactChannel	Concede permissão para criar o canal de comunicação de um contato.	Gravar	contact*		
CreateRotation	Concede permissão para criar uma alternância em uma programação de plantão	Gravar	rotation*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateRotationOverride	Concede permissão para criar uma substituição de alternância em uma programação de plantão	Gravar	rotation*		
DeactivateContactChannel	Concede permissão para desabilitar o canal de comunicação de um contato.	Write	contactchannel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteContact	Concede permissão para excluir um contato.	Write	contact*		
DeleteContactChannel	Concede permissão para excluir o canal de comunicação de um contato.	Gravar	contactchannel*		
DeleteRotation	Concede permissão para excluir uma alternância	Gravar	rotation*		
DeleteRotationOverride	Concede permissão para excluir uma substituição de alternância da alternância	Gravar	rotation*		
DescribeEngagement	Concede permissão para descrever uma interação.	Read	engagement*		
DescribePage	Concede permissão para descrever uma página.	Read	page*		
GetContact	Concede permissão para obter um contato.	Read	contact*		
GetContactChannel	Concede permissão para obter o canal de um contato.	Leitura	contactchannel*		
GetContactPolicy	Concede permissão para obter a política de recursos de um contato	Leitura	contact*		
GetRotation	Concede permissão para recuperar informações sobre uma alternância de plantão	Leitura	rotation*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetRotationOverride	Concede permissão para recuperar informações sobre uma substituição em uma alternância de plantão	Leitura	rotation*		
ListContactChannels	Concede permissão para listar todos os canais de comunicação de um contato.	List	contact*		
ListContacts	Concede permissão para listar todos os contatos.	List			
ListEngagements	Concede permissão para listar todas as interações.	List			
ListPageReceipts	Concede permissão para listar todos os recibos de uma página.	Lista	page*		
ListPageResolutions	Concede permissão para listar o caminho de resolução de uma interação	Lista	page*		
ListPagesByContact	Concede permissão para listar todas as páginas enviadas a um contato.	List	contact*		
ListPagesByEngagement	Concede permissão para listar todas as páginas criadas em uma interação.	Lista	engagement*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListPreviewRotationShifts	Concede permissão para recuperar uma lista de turnos com base nos parâmetros de configuração de alternância	Lista			
ListRotationOverrides	Concede permissão para recuperar uma lista de substituições especificadas atualmente para uma alternância de plantão	Lista	rotation*		
ListRotationShifts	Concede permissão para recuperar uma lista de turnos de alternância em uma programação de plantão	Lista	rotation*		
ListRotations	Concede permissão para recuperar uma lista de alternâncias de plantão	Lista			
ListTagsForResource	Concede permissão para visualizar uma lista de etiquetas de recursos para um recurso especificado	Leitura	contact rotation		
PutContactPolicy	Concede permissão para adicionar uma política de recursos a um contato.	Write	contact*		
SendActivationCode	Concede permissão para enviar o código de ativação do canal de comunicação de um contato.	Write	contactchannel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartEngagement	Concede permissão para iniciar uma interação.	Write	contact*		
StopEngagement	Concede permissão para interromper uma interação.	Gravar	engagement*		
TagResource	Concede permissão para adicionar tags ao recurso especificado	Tags	contact		
			rotation		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover tags do recurso especificado	Tags	contact		
			rotation		
				aws:TagKeys	
UpdateContact	Concede permissão para atualizar um contato.	Write	contact*		ssm-contacts:AssociateContact
UpdateContactChannel	Concede permissão para atualizar o canal de comunicação de um contato.	Gravar	contactchannel*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateRotation	Concede permissão para atualizar as informações especificadas de uma alternância de plantão	Gravar	rotation*		

Tipos de recurso definidos pelo AWS Systems Manager Incident Manager Contacts

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
contact	`arn:${Partition}:ssm-contacts:${Region}:${Account}:contact/${ContactAlias}`	aws:ResourceTag/${TagKey}
contactchannel	`arn:${Partition}:ssm-contacts:${Region}:${Account}:contactchannel/${ContactAlias}/${ContactChannelId}`	
engagement	`arn:${Partition}:ssm-contacts:${Region}:${Account}:engagement/${ContactAlias}/${EngagementId}`	
page	`arn:${Partition}:ssm-contacts:${Region}:${Account}:page/${ContactAlias}/${PageId}`	

Tipos de recursos	ARN	Chaves de condição
rotation	`arn:${Partition}:ssm-contacts:${Region}:${Account}:rotation/${RotationId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Systems Manager Incident Manager Contacts

AWS Os contatos do Systems Manager Incident Manager definem as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição da Configuração Rápida do AWS Systems Manager

AWS O Systems Manager Quick Setup (prefixo do serviço:`ssm-quicksetup`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Configuração Rápida do AWS Systems Manager
- Tipos de recursos definidos pela Configuração Rápida do AWS Systems Manager
- Chaves de condição da Configuração Rápida do AWS Systems Manager

Ações definidas pela Configuração Rápida do AWS Systems Manager

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateConfigurationManager	Concede permissão para criar um recurso do gerenciador de configuração da Configuração Rápida	Gravar	configuration-manager*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteConfigurationManager	Concede permissão para excluir um gerenciador de configurações	Gravar	configuration-manager*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetConfiguration	Concede permissão para obter a configuração do Quick Setup	Leitura	configuration-manager		
GetConfigurationManager	Concede permissão para obter um gerenciador de configuração	Leitura	configuration-manager*		
GetServiceSettings	Concede permissão para definir as configurações da Configuração rápida na solicitação Conta da AWS e Região da AWS	Leitura			
ListConfigurationManagers	Concede permissão para listar os gerenciadores de configuração da Configuração Rápida	Lista			
ListConfigurations	Concede permissão para listar as configurações do Quick Setup	Lista	configuration-manager		
ListQuickSetupTypes	Concede permissão para listar os tipos de Configuração Rápida disponíveis	Leitura			
ListTagsForResource	Concede permissão para listar as tags atribuídas ao recurso	Leitura	configuration-manager*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para atribuir pares de metadados de valores-chave aos recursos AWS	Tags	configuration-manager*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover tags do recurso especificado	Tags	configuration-manager*		
				aws:TagKeys	
UpdateConfigurationDefinition	Concede permissão para atualizar uma definição de configuração da Configuração Rápida	Gravar	configuration-manager*		
UpdateConfigurationManager	Concede permissão para atualizar um gerenciador de configuração da Configuração Rápida	Gravar	configuration-manager*		
UpdateServiceSettings	Concede permissão para atualizar as configurações da Configuração Rápida	Gravar			

Tipos de recursos definidos pela Configuração Rápida do AWS Systems Manager

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
configuration-manager	`arn:${Partition}:ssm-quicksetup:${Region}:${Account}:configuration-manager/${ConfigurationManagerId}`	aws:ResourceTag/${TagKey}

Chaves de condição da Configuração Rápida do AWS Systems Manager

AWS O Systems Manager Quick Setup define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String

Chaves de condição	Descrição	Tipo
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o Tag Editor

O Tag Editor (prefixo do serviço: `resource-explorer`) fornece os recursos, ações e chaves de contexto de condição a seguir específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Tag Editor
- Tipos de recursos definidos pelo Tag Editor
- Chaves de condição do Tag Editor

Ações definidas pelo Tag Editor

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListResourceTypes [somente permissão]	Concede permissão para recuperar os tipos de recursos atualmente compatíveis com o Tag Editor	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListResources [somente permissão]	Concede permissão para recuperar os identificadores dos recursos no Conta da AWS	Lista			
ListTags [somente permissão]	Concede permissão para recuperar as etiquetas anexadas aos identificadores de recursos especificados	Read			tag:GetResources

Tipos de recursos definidos pelo Tag Editor

O Tag Editor não oferece suporte à especificação do ARN de um recurso no elemento `Resource` de uma instrução de política do IAM. Para permitir o acesso ao Tag Editor, especifique `"Resource": "*"` na política.

Chaves de condição do Tag Editor

O Tag Editor não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para o AWS Tax Settings

AWS As configurações fiscais (prefixo do serviço:`tax`) fornecem os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Tax Settings
- Tipos de recursos definidos pelo AWS Tax Settings
- Chaves de condição do AWS Tax Settings

Ações definidas pelo AWS Tax Settings

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchDeleteTaxRegistration	Concede permissão para excluir em lote os dados de registro fiscal	Gravar			
BatchPutTaxRegistration	Concede permissão para atualizar em lote os registros fiscais	Gravar			
DeleteSupplementalTaxRegistration	Concede permissão para excluir dados cadastrais fiscais complementares	Gravar			
DeleteTaxRegistration	Concede permissão para excluir dados de registro fiscal	Gravar			
GetExemptions	Concede permissão para visualizar dados de isenções fiscais	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetTaxInfoReportingDocument [somente permissão]	Concede permissão para view/download documentos/formulários fiscais	Leitura			
GetTaxInheritance	Concede permissão para visualizar o status de herança fiscal	Leitura			
GetTaxInterview [somente permissão]	Concede permissão para recuperar dados de entrevista fiscal	Leitura			
GetTaxRegistration	Concede permissão para exibir dados de registros fiscais	Leitura			
GetTaxRegistrationDocument	Concede permissão para baixar documentos de registro fiscal	Leitura			
ListSupplementalTaxRegistrations	Concede permissão para visualizar registros fiscais complementares	Leitura			
ListTaxRegistrations	Concede permissão para visualizar registros fiscais	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutSupplementalTaxRegistration	Concede permissão para atualizar dados de registros fiscais complementares	Gravar			
PutTaxInheritance	Concede permissão para definir a herança fiscal	Gravar			
PutTaxInterview [somente permissão]	Concede permissão para atualizar dados de entrevista fiscal	Gravar			
PutTaxRegistration	Concede permissão para atualizar dados de registros fiscais	Gravar			
UpdateExemptions	Concede permissão para atualizar dados de isenções fiscais	Gravar			

Tipos de recursos definidos pelo AWS Tax Settings

AWS As configurações fiscais não oferecem suporte à especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para conceder acesso ao AWS Tax Settings, especifique `"Resource": "*"` na política.

Chaves de condição do AWS Tax Settings

O Tax Settings não tem chaves de contexto específicas do serviço que possam ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS Telco Network Builder

AWS O Telco Network Builder (prefixo do serviço:`tnb`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Telco Network Builder
- Tipos de recursos definidos pelo AWS Telco Network Builder
- Chaves de condição do AWS Telco Network Builder

Ações definidas pelo AWS Telco Network Builder

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelSolNetworkOperation	Concede permissão para cancelar uma operação de rede	Gravar	network-operation*		
CreateSolFunctionPackage	Concede permissões para criar um pacote de função	Gravar	function-package*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSolNetworkInstance	Concede permissão para criar uma instância de rede	Gravar	network-instance*		
			network-package*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSolNetworkPackage	Concede permissão para criar um pacote de rede	Gravar	network-package*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSolFunctionPackage	Concede permissão para excluir um pacote de função	Gravar	function-package*		
DeleteSolNetworkInstance	Concede permissão para excluir uma instância de rede	Gravar	network-instance*		
DeleteSolNetworkPackage	Concede permissão para excluir um pacote de rede	Gravar	network-package*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSolFunctionInstance	Concede permissão para obter uma instância de função	Leitura	function-instance*		
				aws:ResourceTag/${TagKey}	
GetSolFunctionPackage	Concede permissão para obter um pacote de função	Leitura	function-package*		
				aws:ResourceTag/${TagKey}	
GetSolFunctionPackageContent	Concede permissão para obter conteúdo de pacotes de função	Leitura	function-package*		
				aws:ResourceTag/${TagKey}	
GetSolFunctionPackageDescriptor	Concede permissão para obter um descritor de pacotes de função	Leitura	function-package*		
				aws:ResourceTag/${TagKey}	
GetSolNetworkInstance	Concede permissão para obter uma instância de rede	Leitura	network-instance*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSolNetworkOperation	Concede permissão para obter uma operação de rede	Leitura	network-operation*		
				aws:ResourceTag/${TagKey}	
GetSolNetworkPackage	Concede permissão para obter um pacote de rede	Leitura	network-package*		
				aws:ResourceTag/${TagKey}	
GetSolNetworkPackageContent	Concede permissão para obter conteúdo de pacotes de rede	Leitura	network-package*		
				aws:ResourceTag/${TagKey}	
GetSolNetworkPackageDescriptor	Concede permissão para obter um descritor de pacotes de rede	Leitura	network-package*		
				aws:ResourceTag/${TagKey}	
InstantiateSolNetworkInstance	Concede permissão para instanciar uma instância de rede	Gravar	network-instance*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
ListSolFunctionInstances	Concede permissão para listar instâncias de função	Lista	function-instance*		
				aws:ResourceTag/${TagKey}	
ListSolFunctionPackages	Concede permissão para listar pacotes de função	Lista	function-package*		
				aws:ResourceTag/${TagKey}	
ListSolNetworkInstances	Concede permissão para listar instâncias de rede	Lista	network-instance*		
				aws:ResourceTag/${TagKey}	
ListSolNetworkOperations	Concede permissão para listar operações de rede	Lista	network-operation*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
ListSolNetworkPackages	Concede permissão para listar pacotes de rede	Lista	network-package*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource	Concede permissão para retornar uma lista de etiquetas de um recurso	Lista			
PutSolFunctionPackageContent	Concede permissão para carregar conteúdo de pacotes de função	Gravar	function-package*		
PutSolNetworkPackageContent	Concede permissão para carregar conteúdo de pacotes de rede	Gravar	network-package*		
TagResource	Concede permissão para adicionar tags ao recurso especificado	Tags	function-instance		
			function-package		
			network-instance		
			network-operation		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			network-package		
				aws:TagKeys aws:RequestTag/${TagKey}	
TerminateSolNetworkInstance	Concede permissão para encerrar uma instância de rede	Gravar	network-instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover tags do recurso especificado	Tags	function-instance		
			function-package		
			network-instance		
			network-operation		
			network-package		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys	
UpdateSolFunctionPackage	Concede permissão para atualizar um pacote de função	Gravar	function-package*		
UpdateSolNetworkInstance	Concede permissão para atualizar uma instância de rede	Gravar	function-instance*		
			network-instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateSolNetworkPackage	Concede permissão para atualizar um pacote de rede	Gravar	network-package*		
ValidateSolFunctionPackageContent	Concede permissão para validar conteúdo de pacotes de função	Gravar	function-package*		
ValidateSolNetworkPackageContent	Concede permissão para validar conteúdo de pacotes de rede	Gravar	network-package*		

Tipos de recursos definidos pelo AWS Telco Network Builder

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS Telco Network Builder

AWS O Telco Network Builder define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso verificando a presença de pares de chave-valor de etiquetas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso verificando pares de chave-valor de etiquetas anexadas ao recurso	String
aws:TagKeys	Filtra acesso pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Textract

O Amazon Textract (prefixo do serviço: `textract`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Textract
- Tipos de recursos definidos pelo Amazon Textract
- Chaves de condição do Amazon Textract

Ações definidas pelo Amazon Textract

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando

usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AnalyzeDocument	Concede permissão para detectar instâncias de entidades de documentos do mundo real em uma imagem fornecida como entrada	Leitura			s3:GetObject
AnalyzeExpense	Concede permissão para detectar instâncias de entidades de documentos do mundo real em uma imagem fornecida como entrada	Leitura			s3:GetObject
AnalyzeID	Concede permissão para detectar informações relevantes de documentos de identidade fornecidos como entrada	Leitura			s3:GetObject
CreateAdapter	Concede permissão para criar um adaptador do Amazon Textract	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAdapterVersion	Concede permissão para criar uma versão do adaptador do Amazon Textract	Gravar	adapter*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteAdapter	Concede permissão para excluir um adaptador do Amazon Textract	Gravar	adapter*		
DeleteAdapterVersion	Concede permissão para excluir uma versão do adaptador do Amazon Textract	Gravar	adapterversion*		
DetectDocumentText	Concede permissão para detectar texto em documentos de imagens	Leitura			s3:GetObject
GetAdapter	Concede permissão para obter um adaptador do Amazon Textract	Leitura	adapter*		
GetAdapterVersion	Concede permissão para obter uma versão do adaptador do Amazon Textract	Leitura	adapterversion*		
GetDocumentAnalysis	Concede permissão para retornar informações sobre um trabalho de análise de documento	Leitura			
GetDocumentTextDetection	Concede permissão para retornar informações sobre um trabalho de detecção de texto de um documento	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetExpenseAnalysis	Concede permissão para retornar informações sobre um experimento	Leitura			
GetLendingAnalysis	Concede permissão para recuperar informações em nível de página sobre um trabalho de análise de empréstimos	Leitura			
GetLendingAnalysisSummary	Concede permissão para recuperar informações resumidas sobre um trabalho de análise de empréstimos	Leitura			
ListAdapterVersions	Concede permissão para listar versões do adaptador do Amazon Textract	Leitura			
ListAdapters	Concede permissão para listar adaptadores do Amazon Textract	Leitura			
ListTagsForResource	Concede permissão para retornar uma lista de etiquetas associadas a um recurso	Leitura	adapter		
			adapterversion		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartDocumentAnalysis	Concede permissão para iniciar um trabalho assíncrono para detectar instâncias de entidades de documentos do mundo real dentro de uma imagem ou pdf fornecido como entrada	Gravar			s3:GetObject
StartDocumentTextDetection	Concede permissão para iniciar um trabalho assíncrono para detectar texto em imagens ou pdfs de documentos	Gravar			s3:GetObject
StartExpenseAnalysis	Concede permissão para iniciar um trabalho assíncrono para detectar instâncias de invoices ou recibos dentro de uma imagem ou pdf fornecido como entrada	Gravar			s3:GetObject
StartLendingAnalysis	Concede permissão para iniciar um trabalho assíncrono para detectar entidades em um documento de empréstimo, obtido a partir de uma imagem ou de um PDF fornecido como entrada	Gravar			s3:GetObject
TagResource	Concede permissão para adicionar uma ou mais etiquetas a um recurso	Marcação	adapter adapterversion		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover uma ou mais etiquetas de um recurso	Tags	adapter		
			adapterversion		
				aws:TagKeys	
UpdateAdapter	Concede permissão para atualizar o adaptador do Amazon Textract	Gravar	adapter*		

Tipos de recursos definidos pelo Amazon Textract

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
adapter	`arn:${Partition}:textract:${Region}:${Account}:/adapters/${AdapterId}`	aws:ResourceTag/${TagKey}
adapterversion	`arn:${Partition}:textract:${Region}:${Account}:/adapters/${AdapterId}/versions/${AdapterVersion}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Textract

O Amazon Textract define as chaves de condição a seguir que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves de etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o Amazon Timestream

O Amazon Timestream (prefixo de serviço: `timestream`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de IAM permissão.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Timestream
- Tipos de recursos definidos pelo Amazon Timestream
- Chaves de condição para o Amazon Timestream

Ações definidas pelo Amazon Timestream

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CancelQuery	Concede permissão para cancelar consultas na conta	Gravar			timestream:DescribeEndpoints
CreateBatchLoadTask	Concede permissão para criar uma tarefa de carregamento em lote em sua conta	Gravar	table*		timestream:DescribeEndpoints timestream:WriteRecords
CreateDatabase	Concede permissão para criar um banco de dados na conta	Gravar	database*		timestream:Describ

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					eEndpoints
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateScheduledQuery	Concede permissão para criar uma nova consulta programada em sua conta	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole timestream:DescribeEndpoints
CreateTable	Concede permissão para criar uma tabela na sua conta	Gravar	table*		timestream:DescribeEndpoints
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDatabase	Concede permissão para excluir um banco de dados na conta	Gravar	database*		timestream:DescribeEndpoints

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteScheduledQuery	Concede permissão para excluir uma consulta programada em sua conta	Gravar	scheduled-query*		timestream:DescribeEndpoints
DeleteTable	Concede permissão para excluir uma tabela na conta	Gravar	table*		timestream:DescribeEndpoints
DescribeAccountSettings	Concede permissão para descrever as configurações da conta	Leitura			timestream:DescribeEndpoints
DescribeBatchLoadTask	Concede permissão para descrever uma tarefa de carregamento em lote em sua conta	Leitura			timestream:DescribeEndpoints
DescribeDatabase	Concede permissão para descrever um banco de dados na conta	Leitura	database*		timestream:DescribeEndpoints
DescribeEndpoints	Concede permissão para descrever endpoints do Timestream	Lista			
DescribeScheduledQuery	Concede permissão para descrever uma consulta programada em sua conta	Leitura	scheduled-query*		timestream:DescribeEndpoints

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeTable	Concede permissão para descrever uma tabela em sua conta	Leitura	table*		timestream:DescribeEndpoints
ExecuteScheduledQuery	Concede permissão para executar uma consulta agendada em sua conta	Gravar	scheduled-query*		timestream:DescribeEndpoints
GetAwsBackupStatus	Concede permissão para obter o status de um backup de tabela do Timestream	Leitura			timestream:DescribeEndpoints
GetAwsRestoreStatus	Concede permissão para obter o status de uma recuperação de tabela do Timestream	Leitura			timestream:DescribeEndpoints
ListBatchLoadTasks	Concede permissão para listar tarefas de carregamento em lote em sua conta	Lista			timestream:DescribeEndpoints
ListDatabases	Concede permissão para listar bancos de dados em sua conta	Lista			timestream:DescribeEndpoints

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListMeasures	Concede permissão para listar medidas de uma tabela em sua conta	Lista	table*		timestream:DescribeEndpoints
ListScheduledQueries	Concede permissão para listar consultas programadas em sua conta	Lista			timestream:DescribeEndpoints
ListTables	Concede permissão para listar tabelas em sua conta	Lista	database*		timestream:DescribeEndpoints
ListTagsForResource	Concede permissão para listar etiquetas de um recurso em sua conta	Leitura	database*		timestream:DescribeEndpoints
			scheduled-query*		
			table*		
PrepareQuery	Concede permissão para emitir consultas de preparação	Leitura	table*		timestream:DescribeEndpoints timestream:Select

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ResumeBatchLoadTask	Concede permissão para retomar uma tarefa de carregamento em lote em sua conta	Gravar			timestream:DescribeEndpoints timestream:WriteRecords
Select	Concede permissão para emitir consultas do tipo “SELECT FROM tabela”	Leitura	table*		timestream:DescribeEndpoints
SelectValues	Concede permissão para emitir consultas do tipo “SELECT 1”	Leitura			timestream:DescribeEndpoints
StartAwsBackupJob	Concede permissão para iniciar um trabalho de backup de uma tabela do Timestream	Gravar	table*		timestream:DescribeEndpoints
StartAwsRestoreJob	Concede permissão para iniciar um trabalho de restauração de uma tabela de backup do Timestream	Gravar	table*		timestream:DescribeEndpoints
TagResource	Concede permissão para adicionar tags a um recurso	Tags	database*		timestream:DescribeEndpoints

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			scheduled-query*		
			table*		
				aws:RequestTag/${TagKey} aws:TagKeys	
Unload	Concede permissão para emitir consultas de descarregamento	Gravar	table*		s3:AbortMultipartUpload s3:GetObject s3:PutObject timestream:DescribeEndpoints timestream:Select
UntagResource	Concede permissão para remover uma etiqueta de um recurso	Tags	database*		timestream:DescribeEndpoints

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			scheduled-query*		
			table*		
				aws:TagKeys	
UpdateAccountSettings	Concede permissão para atualizar as configurações da conta	Gravar			timestream:DescribeEndpoints
UpdateDatabase	Concede permissão para atualizar um banco de dados em sua conta	Gravar	database*		timestream:DescribeEndpoints
UpdateScheduledQuery	Concede permissão para excluir uma consulta programada em sua conta	Gravar	scheduled-query*		timestream:DescribeEndpoints
UpdateTable	Concede permissão para atualizar uma tabela em sua conta	Gravar	table*		timestream:DescribeEndpoints
WriteRecords	Concede permissão para inserir dados em uma tabela em sua conta	Gravar	table*		timestream:DescribeEndpoints

Tipos de recursos definidos pelo Amazon Timestream

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição para o Amazon Timestream

O Amazon Timestream define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma IAM política. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon Timestream InfluxDB

O Amazon Timestream InfluxDB (prefixo do serviço: `timestream-influxdb`) fornece os recursos, ações e chaves de contexto de condição a seguir específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Timestream InfluxDB
- Tipos de recursos definidos pelo Amazon Timestream InfluxDB
- Chaves de condição do Amazon Timestream InfluxDB

Ações definidas pelo Amazon Timestream InfluxDB

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou

ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateDbCluster	Concede permissão para criar um novo cluster Timestream InfluxDB	Gravar	db-parameter-group		timestream-influxdb:CreateDbInstance
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDbInstance	Concede permissão para criar uma instância do Timestream InfluxDB	Gravar	db-parameter-group		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDbParameterGroup	Concede permissão para criar um grupo de parâmetros do Timestream InfluxDB	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDbCluster	Concede permissão para excluir um cluster Timestream InfluxDB	Gravar	db-cluster*		timestream-influxdb:DeleteD

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					bInstance
DeleteDbInstance	Concede permissão para excluir uma instância do Timestream InfluxDB	Gravar	db-instance*		
GetDbCluster	Concede permissão para obter informações sobre um cluster Timestream InfluxDB	Leitura	db-cluster*		
GetDbInstance	Concede permissão para obter informações sobre uma instância do Timestream InfluxDB	Leitura	db-instance*		
GetDbParameterGroup	Concede permissão para obter informações sobre um grupo de parâmetros do Timestream InfluxDB	Leitura	db-parameter-group*		
ListDbClusters	Concede permissão para listar informações sobre todos os clusters do Timestream InfluxDB na conta	Lista			
ListDbInstances	Concede permissão para listar informações sobre todas as instâncias do Timestream InfluxDB na conta	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDbInstancesForCluster	Concede permissão para listar informações sobre todas as instâncias do Timestream InfluxDB pertencentes a um cluster	Leitura	db-cluster*		
ListDbParameterGroups	Concede permissão para listar informações sobre todos os grupos de parâmetros do Timestream InfluxDB	Lista			
ListTagsForResource	Concede permissão para listar as tags de um recurso do Timestream InfluxDB	Leitura	db-cluster		
			db-instance		
			db-parameter-group		
				aws:ResourceTag/${TagKey}	
TagResource	Concede permissão para marcar um recurso do Timestream InfluxDB	Tags	db-cluster		
			db-instance		
			db-parameter-group		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso do Timestream InfluxDB	Tags	db-cluster		
			db-instance		
			db-parameter-group		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateDbCluster	Concede permissão para atualizar um cluster Timestream InfluxDB	Gravar	db-cluster*		timestream-influxdb:UpdateDbInstance

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			db-parameter-group		
UpdateDbInstance	Concede permissão para atualizar uma instância do Timestream InfluxDB	Gravar	db-instance*		
			db-parameter-group		

Tipos de recursos definidos pelo Amazon Timestream InfluxDB

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
db-parameter-group	`arn:${Partition}:timestream-influxdb:${Region}:${Account}:db-parameter-group/${DbParameterGroupIdentifier}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Timestream InfluxDB

O Amazon Timestream InfluxDB define as chaves de condição a seguir que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por um par de chave valor da etiqueta que é permitido na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso por um par de chave e valor da etiqueta de um recurso.	Segmento
aws:TagKeys	Filtra o acesso por uma lista de chaves da etiqueta que são permitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Tiros

AWS Tiros (prefixo do serviço:`tiros`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Tiros
- Tipos de recursos definidos pelo AWS Tiros
- Chaves de condição do AWS Tiros

Ações definidas pelo AWS Tiros

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de

condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateQuery [somente permissão]	Concede permissão para criar uma consulta de acessibilidade da VPC	Write			
ExtendQuery [somente permissão]	Concede permissão para ampliar uma consulta de acessibilidade da VPC para incluir a conta das entidades principais da chamada	Gravar			
GetQueryAnswer [somente permissão]	Concede permissão para obter respostas de consulta de acessibilidade da VPC	Read			
GetQueryExplanation [somente permissão]	Concede permissão para obter explicações de consulta de acessibilidade da VPC	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetQueryExtensionAccounts [somente permissão]	Concede permissão para listar contas que podem ser úteis em uma nova consulta	Leitura			

Tipos de recursos definidos pelo AWS Tiros

AWS O Tiros não suporta a especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para permitir acesso ao AWS Tiros, especifique `"Resource": "*"` na política.

Chaves de condição do AWS Tiros

O Tiros não tem chaves de contexto específicas do serviço que possam ser usadas no elemento `Condition` de instruções da política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do Amazon Transcribe

O Amazon Transcribe (prefixo do serviço: `transcribe`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Transcribe
- Tipos de recursos definidos pelo Amazon Transcribe

- Chaves de condição do Amazon Transcribe

Ações definidas pelo Amazon Transcribe

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui

a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateCallAnalyticsCategory	Concede permissão para criar uma categoria de analytics. O Amazon Transcribe aplica as condições especificadas por suas categorias de analytics aos trabalhos de analytics de chamadas	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateLanguageModel	Concede permissão para criar um modelo de idioma personalizado	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject s3:ListBucket
CreateMedicalVocabulary	Concede permissão para criar um vocabulário personalizado que pode ser usado para alterar a forma como o Amazon Transcribe Medical	Write		aws:RequestTag/${TagKey}	s3:GetObject

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	lida com a transcrição de um arquivo de áudio			aws:ResourceTag/${TagKey} aws:TagKeys	
CreateVocabulary	Concede permissão para criar um vocabulário personalizado que pode ser usado para alterar a forma como o Amazon Transcribe lida com a transcrição de um arquivo de áudio	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject
CreateVocabularyFilter	Concede permissão para criar um filtro de vocabulário que pode ser usado para excluir do filtro palavras da transcrição de um arquivo de áudio gerado pelo Amazon Transcribe	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject
DeleteCallAnalyticsCategory	Concede permissão para excluir uma categoria de analytics de chamada usando seu nome do Amazon Transcribe	Write	callanalyticscategory*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteCallAnalyticsJob	Concede permissão para excluir um trabalho de analytics enviado anteriormente com qualquer outro resultado gerado, como a transcrição, os modelos e assim por diante	Write	callanalyticsjob*		
DeleteLanguageModel	Concede permissão para excluir um modelo de idioma personalizado criado anteriormente	Gravar	languagemodel*		
DeleteMedicalScribeJob	Concede permissão para excluir um trabalho de Transcrição médica enviado anteriormente	Gravar	medicalscribejob*		
DeleteMedicalTranscriptionJob	Concede permissão para excluir um trabalho de transcrição médica enviado anteriormente	Write	medicaltranscriptionjob*		
DeleteMedicalVocabulary	Concede permissão para excluir um vocabulário médico do Amazon Transcribe	Write	medicalvocabulary*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteTranscriptionJob	Concede permissão para excluir um trabalho de transcrição enviado anteriormente com qualquer outro resultado gerado, como a transcrição, os modelos e assim por diante	Write	transcriptionjob*		
DeleteVocabulary	Concede permissão para excluir um vocabulário do Amazon Transcribe	Write	vocabulary*		
DeleteVocabularyFilter	Concede permissão para excluir um filtro de vocabulário do Amazon Transcribe	Write	vocabularyfilter*		
DescribeLanguageModel	Concede permissão para retornar informações sobre um modelo de idioma personalizado	Read	languagemodel*		
GetCallAnalyticsCategory	Concede permissão para recuperar informações sobre uma categoria de analytics de chamadas	Read	callanalyticscategory*		
GetCallAnalyticsJob	Concede permissão para retornar informações sobre um trabalho de analytics de chamadas	Leitura	callanalyticsjob*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetMedicalScribeJob	Concede permissão para retornar informações sobre um trabalho de Transcrição médica	Leitura	medicalscribejob*		
GetMedicalScribeStream	Concede permissão para obter informações sobre a sessão AWS HealthScribe de streaming especificada	Leitura			
GetMedicalTranscriptionJob	Concede permissão para retornar informações sobre um trabalho de transcrição médica	Read	medicaltranscriptionjob*		
GetMedicalVocabulary	Concede permissão para obter informações sobre um vocabulário médico	Read	medicalvocabulary*		
GetTranscriptionJob	Concede permissão para retornar informações sobre um trabalho de transcrição	Read	transcriptionjob*		
GetVocabulary	Concede permissão para obter informações sobre um vocabulário	Read	vocabulary*		
GetVocabularyFilter	Concede permissão para obter informações sobre um filtro de vocabulário	Read	vocabularyfilter*		
ListCallAnalyticsCategories	Concede permissão para listar categorias de analytics de chamadas que foram criadas	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListCallAnalyticsJobs	Concede permissão para listar trabalhos de analytics de chamadas com o status especificado	List			
ListLanguageModels	Concede permissão para listar modelos de idioma personalizados	Lista			
ListMedicalScribeJobs	Concede permissão para listar trabalhos de Transcrição médica com o status especificado	Lista			
ListMedicalTranscriptionJobs	Concede permissão para listar trabalhos de transcrição médica com o status especificado	List			
ListMedicalVocabularies	Concede permissão para retornar uma lista de vocabulários médicos que correspondem aos critérios especificados. Se não houver critérios especificados, retornará toda a lista de vocabulários	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTranscriptionJobs	Concede permissão para listar trabalhos de transcrição com o status especificado	List			
ListVocabularies	Concede permissão para retornar uma lista de vocabulários que correspondem aos critérios especificados. Se não houver critérios especificados, retornará toda a lista de vocabulários	List			
ListVocabularyFilters	Concede permissão para retornar uma lista de filtros de vocabulário que correspondam aos critérios especificados. Se não houver critérios especificados, retornará no máximo 5 filtros de vocabulário	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartCallAnalyticsJob	Concede permissão para iniciar um trabalho de analytics assíncrono que não só transcreve a gravação de áudio de um chamador e agente, mas também retorna insights adicionais	Gravar		transcribe:OutputEncryptionKMSKeyId transcribe:OutputLocation aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
StartCallAnalyticsStreamTranscription	Concede permissão para iniciar um protocolo em que o áudio é transmitido para o Transcribe Call Analytics e os resultados da transcrição são transmitidos para sua aplicação	Gravar			
StartCallAnalyticsStreamTranscriptionWebSocket	Concede permissão para iniciar um WebSocket onde o áudio é transmitido para o Transcribe Call Analytics e os resultados da transcrição são transmitidos para seu aplicativo	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartMedicalScribeJob	Concede permissão para iniciar um trabalho assíncrono para transcrever conversas entre paciente e médico e gerar notas clínicas	Gravar		transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject
StartMedicalScribeStream	Concede permissão para iniciar um HTTP2 fluxo bidirecional no qual o áudio é transmitido AWS HealthScribe e os resultados da transcrição são transmitidos para seu aplicativo	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartMedicalStreamTranscription	Concede permissão para iniciar um protocolo em que o áudio é transmitido para o Transcribe Medical e os resultados da transcrição são transmitidos para sua aplicação	Gravar			
StartMedicalStreamTranscriptionWebSocket	Concede permissão para iniciar um WebSocket onde o áudio é transmitido para o Transcribe Medical e os resultados da transcrição são transmitidos para seu aplicativo	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartMedicalTranscriptionJob	Concede permissão para iniciar um trabalho assíncrono para transcrever fala médica em texto	Gravar		transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId transcribe:OutputKey aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject
StartStreamTranscription	Concede permissão para iniciar um HTTP2 fluxo bidirecional para transcrever fala em texto em tempo real	Gravar			
StartStreamTranscriptionWebSocket	Concede permissão para iniciar uma transmissão de websocket para transcrever fala em texto em tempo real	Write			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartTranscriptionJob	Concede permissão para iniciar um trabalho assíncrono para transcrever fala em texto	Gravar		transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId transcribe:OutputKey aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TagResource	Concede permissão para marcar um recurso com determinados pares de chave-valor	Marcação		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId transcribe:OutputKey aws:TagKeys	
UntagResource	Concede permissão para desmarcar um recurso com determinada chave	Tags		aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateCallAnalyticsCategory	Concede permissão para atualizar a categoria de analytics de chamadas com novos valores. A UpdateCallAnalyticsCategory operação substitui todas as informações existentes pelos valores que você fornece na solicitação	Gravar	callanalyticscategory*		
UpdateMedicalVocabulary	Concede permissão para atualizar um vocabulário médico existente com novos valores. A UpdateMedicalVocabulary operação substitui todas as informações existentes pelos valores que você fornece na solicitação	Gravar	medicalvocabulary*		s3:GetObject
UpdateVocabulary	Concede permissão para atualizar um vocabulário existente com novos valores. A UpdateVocabulary operação substitui todas as informações existentes pelos valores que você fornece na solicitação	Gravar	vocabulary*		s3:GetObject

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateVocabularyFilter	Concede permissão para atualizar um filtro de vocabulário existente com novos valores. A UpdateVocabularyFilter operação substitui todas as informações existentes pelos valores que você fornece na solicitação	Gravar	vocabularyfilter*		s3:GetObject

Tipos de recursos definidos pelo Amazon Transcribe

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
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}

Chaves de condição do Amazon Transcribe

O Amazon Transcribe define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso exigindo valores de etiquetas presentes em uma solicitação de criação de recurso	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelo valor de etiqueta necessário associado ao recurso	String
aws:TagKeys	Filtra o acesso exigindo a presença de etiquetas obrigatórias na solicitação	ArrayOfString
transcribe:OutputBucketName	Filtra o acesso com base no nome do bucket de saída incluído na solicitação	String
transcribe:OutputEncryptionKMSKeyId	Filtra o acesso com base no ID da chave do KMS incluído na solicitação	String
transcribe:OutputKey	Filtra o acesso com base na chave de saída incluída na solicitação	String
transcribe:OutputLocation	Filtra o acesso com base no local de saída incluído na solicitação	String

Ações, recursos e chaves de condição do AWS Transfer Family

AWS Transfer Family (prefixo do serviço:`transfer`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.

- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Transfer Family
- Tipos de recursos definidos pelo AWS Transfer Family
- Chaves de condição do AWS Transfer Family

Ações definidas pelo AWS Transfer Family

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAccess	Concede permissão para adicionar um acesso associado a um servidor	Gravar	server*		iam:PassRole
CreateAgreement	Concede permissão para adicionar um contrato associado a um servidor	Gravar	server*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateConnector	Concede permissão para criar um conector	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	iam:PassRole
CreateProfile	Concede permissão para criar um perfil	Gravar		aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey}	
CreateServer	Concede permissão para criar um servidor	Gravação		aws:TagKeys aws:RequestTag/${TagKey}	iam:PassRole
CreateUser	Concede permissão para adicionar um usuário associado a um servidor	Gravar	server*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateWebApp	Concede permissão para criar um aplicativo web	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	iam:PassRole
CreateWorkflow	Concede permissão para criar um fluxo de trabalho	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteAccess	Concede permissão para excluir acesso	Gravar	server*		
DeleteAgreement	Concede permissão para excluir um contrato	Gravar	agreement*		
DeleteCertificate	Concede permissão para excluir um certificado	Gravar	certificate*		
DeleteConnector	Concede permissão para excluir um conector	Gravar	connector*		
DeleteHostKey	Concede permissão para excluir uma chave de host associada a um servidor	Gravar	host-key*		
DeleteProfile	Concede permissão para excluir perfil	Gravar	profile*		
DeleteServer	Concede permissão para excluir um servidor	Gravação	server*		
DeleteSshPublicKey	Concede permissão para excluir uma chave pública SSH de um usuário	Gravação	user*		
DeleteUser	Concede permissão para excluir um usuário associado a um servidor	Gravar	user*		
DeleteWebApp	Concede permissão para excluir o webapp	Gravar	webapp*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteWebAppCustomization	Concede permissão para excluir a personalização do webapp	Gravar	webapp*		
DeleteWorkflow	Concede permissão para excluir um fluxo de trabalho	Gravar	workflow*		
DescribeAccess	Concede permissão para descrever um acesso atribuído a um servidor	Leitura	server*		
DescribeAgreement	Concede permissão para descrever um contrato atribuído a um servidor	Leitura	agreement*		
DescribeCertificate	Concede permissão para descrever um certificado	Leitura	certificate*		
DescribeConnector	Concede permissão para descrever um conector	Leitura	connector*		
DescribeExecution	Concede permissão para descrever uma execução associada a um fluxo de trabalho	Leitura	workflow*		
DescribeHostKey	Concede permissão para descrever uma chave de host associada a um servidor	Leitura	host-key*		
DescribeProfile	Concede permissão para descrever um perfil	Leitura	profile*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeSecurityPolicy	Concede permissão para descrever uma política de segurança	Read			
DescribeServer	Concede permissão para descrever um servidor	Read	server*		
DescribeUser	Concede permissão para descrever um usuário associado a um servidor	Leitura	user*		
DescribeWebApp	Concede permissão para descrever um aplicativo da web	Leitura	webapp*		
DescribeWebAppCustomization	Concede permissão para descrever a personalização de um aplicativo web	Leitura	webapp*		
DescribeWorkflow	Concede permissão para descrever um fluxo de trabalho	Leitura	workflow*		
ImportCertificate	Concede permissão para adicionar um certificado	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
ImportHostKey	Concede permissão para adicionar uma chave de host a um servidor	Gravar	server*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
ImportSshPublicKey	Concede permissão para adicionar uma chave pública SSH a um usuário	Gravar	user*		
ListAccesses	Concede permissão para listar acessos	Leitura	server*		
ListAgreements	Concede permissão para listar contratos	Leitura	server*		
ListCertificates	Concede permissão para listar certificados	Leitura			
ListConnectors	Concede permissão para listar conectores	Leitura			
ListExecutions	Concede permissão para listar execuções associadas a um fluxo de trabalho	Leitura	workflow*		
ListFileTransferResults	Concede permissão para listar status de transferência de arquivos para conectores	Leitura	connector*		
ListHostKeys	Concede permissão para listar chaves de host associadas a um servidor	Leitura	server*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListProfiles	Concede permissão para listar perfis	Leitura			
ListSecurityPolicies	Concede permissão para listar políticas de segurança	List			
ListServers	Concede permissão para listar servidores	Lista			
ListTagsForResource	Concede permissão para listar tags para um recurso do AWS Transfer Family	Leitura	agreement		
			certificate		
			connector		
			host-key		
			profile		
			server		
			user		
			workflow		
ListUsers	Concede permissão para listar usuários associados a um servidor	Lista	server*		
ListWebApps	Concede permissão para listar aplicativos da web	Lista			
ListWorkflows	Concede permissão para listar fluxos de trabalho	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SendWorkflowStepState	Concede permissão para emitir um retorno de chamada para etapas personalizadas assíncronas	Gravar	workflow*		
StartDirectoryListing	Concede permissão para iniciar uma operação de lista em um servidor remoto usando um conector	Gravar	connector*		
StartFileTransfer	Concede permissão para iniciar uma transferência de arquivo de conexão	Gravar	connector*		
StartRemoteDelete	Concede permissão para iniciar uma operação de exclusão de conectores no servidor remoto	Gravar	connector*		
StartRemoteMove	Concede permissão para iniciar uma operação de movimentação de conectores no servidor remoto	Gravar	connector*		
StartServer	Concede permissão para iniciar um servidor	Write	server*		
StopServer	Concede permissão para interromper um servidor	Gravar	server*		
TagResource	Concede permissão para marcar um recurso do AWS Transfer Family	Tags	agreement certificate		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			connector		
			host-key		
			profile		
			server		
			user		
			webapp		
			workflow		
				aws:TagKeys aws:RequestTag/${TagKey}	
TestConnection	Concede permissão para testar a conexão de um conector com o servidor remoto	Gravar	connector*		
TestIdentityProvider	Concede permissão para testar o provedor de identidade personalizado de um servidor	Leitura	user*		
UntagResource	Concede permissão para desmarcar um recurso do AWS Transfer Family	Tags	agreement		
			certificate		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			connector		
			host-key		
			profile		
			server		
			user		
			webapp		
			workflow		
				aws:TagKeys	
UpdateAccess	Concede permissão para atualizar acesso	Gravar			iam:PassRole
UpdateAgreement	Concede permissão para atualizar um contrato	Gravar	agreement*		iam:PassRole
UpdateCertificate	Concede permissão para atualizar um certificado	Gravar	certificate*		
UpdateConnector	Concede permissão para atualizar um conector	Gravar	connector*		iam:PassRole
UpdateHostKey	Concede permissão para atualizar uma chave de host	Gravar	host-key*		
UpdateProfile	Concede permissão para atualizar um perfil	Gravar	profile*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateServer	Concede permissão para atualizar a configuração de um servidor	Gravação	server*		iam:PassRole
UpdateUser	Concede permissão para atualizar a configuração de um usuário	Gravar	user*		iam:PassRole
UpdateWebApp	Concede permissão para atualizar a configuração de um aplicativo web	Gravar	webapp*		iam:PassRole
UpdateWebAppCustomization	Concede permissão para atualizar a configuração de uma personalização de aplicativo web	Gravar	webapp*		iam:PassRole

Tipos de recursos definidos pelo AWS Transfer Family

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
user	`arn:${Partition}:transfer:${Region}:${Account}:user/${ServerId}/${UserName}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS Transfer Family

AWS A Transfer Family define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para AWS Transform

AWS Transform (prefixo do serviço:`transform`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Transform
- Tipos de recursos definidos pelo AWS Transform
- Chaves de condição para AWS Transform

Ações definidas pelo AWS Transform

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando

usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateConnectorResource [somente permissão]	Concede permissão para invocar AssociateConnectorResource no Transform AWS	Gravar			
CreateProfile [somente permissão]	Concede permissão para invocar CreateProfile no Transform AWS	Gravar	profile*		
DeleteProfile [somente permissão]	Concede permissão para invocar DeleteProfile no Transform AWS	Gravar	profile*		
GetConnector [somente permissão]	Concede permissão para invocar GetConnector no Transform AWS	Leitura			
ListProfiles [somente permissão]	Concede permissão para invocar ListProfiles no Transform AWS	Lista			
RejectConnector [somente permissão]	Concede permissão para invocar RejectConnector no Transform AWS	Gravar			
UpdateProfile [somente permissão]	Concede permissão para invocar UpdateProfile no Transform AWS	Gravar	profile*		

Tipos de recursos definidos pelo AWS Transform

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
profile	`arn:${Partition}:transform:${Region}:${Account}:profile/${Identifier}`	

Chaves de condição para AWS Transform

O Transform não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do Amazon Translate

O Amazon Translate (prefixo do serviço: `translate`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos ao serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Translate
- Tipos de recursos definidos pelo Amazon Translate
- Chaves de condição do Amazon Translate

Ações definidas pelo Amazon Translate

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateParallelData	Concede permissão para criar dados paralelos	Write	parallel-data		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteParallelData	Concede permissão para excluir dados paralelos	Write	parallel-data		
DeleteTerminology	Concede permissão para excluir uma terminologia	Write	terminology		
DescribeTextTranslationJob	Concede permissão para obter as propriedades associadas a um trabalho de tradução em lote assíncrono	Read			
GetParallelData	Concede permissão para obter dados paralelos	Read	parallel-data		
GetTerminology	Concede permissão para recuperar uma terminologia	Read	terminology		
ImportTerminology	Concede permissão para criar ou atualizar uma terminologia, dependendo se já existe ou não uma para o nome de terminologia fornecido	Gravar	terminology		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
ListLanguages	Concede permissão para listar os idiomas compatíveis	Lista			
ListParallelData	Concede permissão para listar Dados paralelos associados à sua conta	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	parallel-data terminology		
ListTerminologies	Concede permissão para listar terminologias associadas à sua conta	List			
ListTextTranslationJobs	Concede permissão para listar trabalhos de tradução em lote que você enviou	List			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartTextTranslationJob	Concede permissão para iniciar um trabalho assíncrono de tradução em lote. Trabalhos de tradução em lote podem ser usados para traduzir grandes volumes de texto em vários documentos de uma só vez	Write	parallel-data		
			terminology		
StopTextTranslationJob	Concede permissão para interromper um trabalho assíncrono de tradução em lote que está em andamento	Gravar			
TagResource	Concede permissão para marcar um recurso com determinados pares de chave-valor	Tags	parallel-data		
			terminology		
				aws:RequestTag/${TagKey} aws:TagKeys	
TranslateDocument	Concede permissão para traduzir um documento de um idioma de origem para um idioma de destino	Leitura	terminology		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
TranslateText	Concede permissão para traduzir texto de um idioma de origem para um idioma de destino	Leitura	parallel-data		
			terminology		
UntagResource	Concede permissão para desmarcar um recurso com determinada chave	Tags	parallel-data		
			terminology		
				aws:TagKeys	
UpdateParallelData	Concede permissão para atualizar dados paralelos existentes	Write	parallel-data		

Tipos de recursos definidos pelo Amazon Translate

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
terminology	`arn:${Partition}:translate:${Region}:${Account}:terminology/${ResourceName}`	aws:ResourceTag/${TagKey}
parallel-data	`arn:${Partition}:translate:${Region}:${Account}:parallel-data/${ResourceName}`	aws:ResourceTag/${TagKey}

Chaves de condição do Amazon Translate

O Amazon Translate define as chaves de condição a seguir que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso exigindo valores de etiquetas presentes em uma solicitação de criação de recurso	String
aws:ResourceTag/${TagKey}	Filtra o acesso pelo valor de etiqueta necessário associado ao recurso	String
aws:TagKeys	Filtra o acesso exigindo a presença de etiquetas obrigatórias na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS Trusted Advisor

AWS O Trusted Advisor (prefixo do serviço:`trustedadvisor`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Trusted Advisor
- Tipos de recursos definidos pelo AWS Trusted Advisor
- Chaves de condição do AWS Trusted Advisor

Ações definidas pelo AWS Trusted Advisor

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar

a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

> **Note**
>
> Os detalhes da descrição da política do IAM Trusted Advisor aplicam-se somente ao console do Trusted Advisor. Se você quiser gerenciar o acesso programático ao Trusted Advisor, use as operações do Trusted Advisor na AWS Support API.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchUpdateRecommendationRe	Concede permissão para atualizar um ou mais status de exclusão para uma lista de recursos de recomendação	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
sourceExclusion					
CreateEngagement	Concede permissão para criar uma interação	Gravar			
CreateEngagementAttachment	Concede permissão para criar um anexo de interação	Gravar			
CreateEngagementCommunication	Concede permissão para criar uma comunicação de interação	Gravar			
DeleteNotificationConfigurationForDelegatedAdmin	Concede permissão à conta de gerenciamento da organização para excluir preferências de notificação por e-mail de uma conta de administrador delegado para o Trusted Advisor Priority	Gravar			
DescribeAccount [somente permissão]	Concede permissão para visualizar o AWS Support plano e várias preferências do AWS Trusted Advisor	Leitura			
DescribeAccountAccess [somente permissão]	Concede permissão para ver se o Conta da AWS habilitou ou desabilitou o AWS Trusted Advisor	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeCheckItems	Concede permissão para visualizar detalhes dos itens de verificação	Leitura	checks*		
DescribeCheckRefreshStatuses	Concede permissão para visualizar os status de atualização das verificações do AWS Trusted Advisor	Leitura	checks*		
DescribeCheckStatusHistoryChanges [somente permissão]	Concede permissão para visualizar os resultados e os status alterados das verificações nos últimos 30 dias	Leitura	checks*		
DescribeCheckSummaries	Concede permissão para visualizar resumos de verificação do AWS Trusted Advisor	Leitura	checks*		
DescribeChecks	Concede permissão para visualizar detalhes das verificações do AWS Trusted Advisor	Leitura			
DescribeNotificationConfigurations	Concede permissão para obter as preferências de notificação por e-mail do Trusted Advisor Priority	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeNotificationPreferences [somente permissão]	Concede permissão para visualizar as preferências de notificação do Conta da AWS	Leitura			
DescribeOrganization [somente permissão]	Concede permissão para ver se o Conta da AWS atende aos requisitos para ativar o recurso de visualização organizacional	Leitura			
DescribeOrganizationAccounts [somente permissão]	Concede permissão para visualizar as AWS contas vinculadas que estão na organização	Leitura			
DescribeReports [somente permissão]	Concede permissão para visualizar detalhes para relatórios de visualização organizacional, como o nome do relatório, o runtime, a data de criação, o status e o formato	Leitura			
DescribeRisk	Concede permissão para visualizar detalhes do risco no AWS Trusted Advisor Priority	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeRiskResources	Concede permissão para visualizar os recursos afetados por um risco no AWS Trusted Advisor Priority	Leitura			
DescribeRisks	Concede permissão para visualizar riscos no AWS Trusted Advisor Priority	Leitura			
DescribeServiceMetadata [somente permissão]	Concede permissão para visualizar informações sobre relatórios de exibição organizacional, como categorias de verificação Regiões da AWS, nomes de cheques e status de recursos	Leitura			
DownloadRisk	Concede permissão para baixar um arquivo que contém detalhes sobre o risco no AWS Trusted Advisor Priority	Leitura			
ExcludeCheckItems [somente permissão]	Concede permissão para excluir recomendações para verificações do AWS Trusted Advisor	Gravar	checks*		
GenerateReport [somente permissão]	Concede permissão para criar um relatório para cheques do AWS Trusted Advisor em sua organização	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetEngagement	Concede permissão para visualizar uma interação	Leitura			
GetEngagementAttachment	Concede permissão para visualizar um anexo de interação	Leitura			
GetEngagementType	Concede permissão para visualizar um tipo de interação específico	Leitura			
GetOrganizationRecommendation	Concede permissão para obter uma recomendação específica dentro da AWS organização de uma organização. Essa API oferece suporte somente a recomendações priorizadas	Leitura			
GetRecommendation	Concede permissão para obter uma recomendação específica	Leitura			
IncludeCheckItems [somente permissão]	Concede permissão para incluir recomendações para verificações do AWS Trusted Advisor	Gravar	checks*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAccountsForParent [somente permissão]	Concede permissão para visualizar, no console do Trusted Advisor, todas as contas em uma AWS organização contidas em uma unidade raiz ou organizacional (OU)	Leitura			
ListChecks	Concede permissão para listar um conjunto filtrável de verificações	Lista			
ListEngagementCommunications	Concede permissão para visualizar todas as comunicações de uma interação	Leitura			
ListEngagementTypes	Concede permissão para visualizar todos os tipos de interação	Leitura			
ListEngagements	Concede permissão para visualizar todas as interações	Leitura			
ListOrganizationRecommendationAccounts	Concede permissão para listar as contas que possuem os recursos para uma recomendação agregada AWS da organização. Essa API oferece suporte somente a recomendações priorizadas	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListOrganizationRecommendationResources	Concede permissão para listar os recursos de uma recomendação dentro de uma AWS organização. Essa API oferece suporte somente a recomendações priorizadas	Lista			
ListOrganizationRecommendations	Concede permissão para listar um conjunto filtrável de recomendações dentro de uma AWS organização. Essa API oferece suporte somente a recomendações priorizadas	Lista			
ListOrganizationalUnitsForParent [somente permissão]	Concede permissão para visualizar, no console do Trusted Advisor, todas as unidades organizacionais (OUs) em uma unidade organizacional principal ou raiz	Leitura			
ListRecommendationResources	Concede permissão para listar recursos de uma recomendação	Lista			
ListRecommendations	Concede permissão para listar um conjunto filtrável de recomendações	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListRoots [somente permissão]	Concede permissão para visualizar, no console do Trusted Advisor, todas as raízes definidas em uma AWS organização	Leitura			
RefreshCheck	Concede permissão para atualizar uma verificação do AWS Trusted Advisor	Gravar	checks*		
SetAccountAccess [somente permissão]	Concede permissão para ativar ou desativar o AWS Trusted Advisor para a conta	Gravar			
SetOrganizationAccess [somente permissão]	Concede permissão para ativar o recurso de visualização organizacional do AWS Trusted Advisor	Gravar			
UpdateEngagement	Concede permissão para atualizar os detalhes de um compromisso	Gravar			
UpdateEngagementStatus	Concede permissão para atualizar o status de uma interação	Gravar			
UpdateNotificationConfigurations	Concede permissão para criar ou atualizar as preferências de notificação por e-mail do Trusted Advisor Priority	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateNotificationPreferences [somente permissão]	Concede permissão para atualizar as preferências de notificação do AWS Trusted Advisor	Gravar			
UpdateOrganizationRecommendationLifecycle	Concede permissão para atualizar o ciclo de vida de uma recomendação dentro de uma organização. AWS Essa API oferece suporte somente a recomendações priorizadas	Gravar			
UpdateRecommendationLifecycle	Concede permissão para atualizar o ciclo de vida de uma recomendação. Essa API oferece suporte somente a recomendações priorizadas	Gravar			
UpdateRiskStatus	Concede permissão para atualizar o status do risco no AWS Trusted Advisor Priority	Gravar			

Tipos de recursos definidos pelo AWS Trusted Advisor

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

> **Note**
>
> O ARN para o tipo de recurso de verificações não deve conter uma região. No formato, em vez de “$ {Region}”, use um “*”, ou a política não funcionará corretamente.

Tipos de recursos	ARN	Chaves de condição
checks	`arn:${Partition}:trustedadvisor:${Region}:${Account}:checks/${CategoryCode}/${CheckId}`	

Chaves de condição do AWS Trusted Advisor

O Trusted Advisor não possui chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do AWS User Notifications

AWS As notificações do usuário (prefixo do serviço:`notifications`) fornecem os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS User Notifications
- Tipos de recursos definidos pelo AWS User Notifications
- Chaves de condição para o AWS User Notifications

Ações definidas pelo AWS User Notifications

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateChannel	Concede permissão para associar um novo canal a um determinado NotificationConfiguration	Gravar	NotificationConfiguration*		
AssociateManagedNotificationAccountContact	Concede permissão para associar um contato da Conta a uma configuração específica de notificação gerenciada	Gravar	ManagedNotificationConfiguration*		
AssociateManagedNotificationAdditionalChannel	Concede permissão para associar um canal a uma configuração específica de notificação gerenciada	Gravar	ManagedNotificationConfiguration*		
CreateEventRule	Concede permissão para criar um novo EventRule, associando-o a um NotificationConfiguration	Gravar			
CreateNotificationConfiguration	Concede permissão para criar um NotificationConfiguration	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteEventRule	Concede permissão para excluir um EventRule	Gravar	EventRule*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteNotificationConfiguration	Concede permissão para excluir um NotificationConfiguration	Gravar	NotificationConfiguration*		
DeregisterNotificationHub	Concede permissão para cancelar o registro de um NotificationHub	Gravar			
DisableNotificationsAccessForOrganization	Concede permissão para desativar o Service Trust para notificações de AWS usuários	Gravar			organizations:DisableAWSServiceAccess
DisassociateChannel	Concede permissão para remover um canal de um NotificationConfiguration	Gravar	NotificationConfiguration*		
DisassociateManagedNotificationAccountContact	Concede permissão para remover um contato da conta de uma configuração de notificação gerenciada	Gravar	ManagedNotificationConfiguration*		
DisassociateManagedNotificationAdditionalChannel	Concede permissão para remover um canal de uma configuração de notificação gerenciada	Gravar	ManagedNotificationConfiguration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
EnableNotificationsAccessForOrganization	Concede permissão para ativar o Service Trust para notificações de AWS usuários	Gravar			iam:CreateServiceLinkedRole organizations:EnableAWSServiceAccess
GetEventRule	Concede permissão para obter um EventRule	Leitura	EventRule*		
GetFeatureOptInStatus [somente permissão]	Concede permissão para ler o status de opt-in de um recurso do Serviço de Notificação AWS do Usuário	Leitura			
GetManagedNotificationChildEvent	Concede permissão para receber um evento secundário de notificação gerenciada	Leitura	ManagedNotificationChildEvent*		
GetManagedNotificationConfiguration	Concede permissão para obter uma configuração de notificação gerenciada	Leitura	ManagedNotificationConfiguration*		
GetManagedNotificationEvent	Concede permissão para obter um Managed NotificationEvent	Leitura	ManagedNotificationEvent*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetNotificationConfiguration	Concede permissão para obter um NotificationConfiguration	Leitura	NotificationConfiguration*		
GetNotificationEvent	Concede permissão para obter um NotificationEvent	Leitura	NotificationEvent*		
GetNotificationsAccessForOrganization	Concede permissão para ler o Service Trust for AWS User Notifications	Leitura			
ListChannels	Concede permissão para listar canais por NotificationConfiguration	Lista	NotificationConfiguration*		
ListEventRules	Concede permissão para listar EventRules	Lista			
ListManagedNotificationChannelAssociations	Concede permissão para listar contatos e canais da conta associados a uma configuração de notificação gerenciada	Lista	ManagedNotificationConfiguration*		
ListManagedNotificationChildEvents	Concede permissão para listar eventos secundários de notificação gerenciada	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListManagedNotificationConfigurations	Concede permissão para listar configurações de notificação gerenciadas	Lista			
ListManagedNotificationEvents	Concede permissão para listar eventos de notificação gerenciados	Lista			
ListNotificationConfigurations	Concede permissão para listar NotificationConfigurations	Lista			
ListNotificationEvents	Concede permissão para listar NotificationEvents	Lista			
ListNotificationHubs	Concede permissão para listar NotificationHubs	Lista			
ListTagsForResource	Concede permissão para obter tags para um recurso	Lista			
PutFeatureOptInStatus [somente permissão]	Concede permissão para atualizar o status de aceitação de um recurso do Serviço de Notificação AWS do Usuário	Gravar			
RegisterNotificationHub	Concede permissão para registrar um NotificationHub	Gravar			
TagResource	Concede permissão para marcar um recurso	Tags	NotificationConfiguration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover etiquetas de um recurso	Tags	NotificationConfiguration*		
				aws:TagKeys	
UpdateEventRule	Concede permissão para atualizar um EventRule	Gravar	EventRule*		
UpdateNotificationConfiguration	Concede permissão para atualizar um NotificationConfiguration	Gravar	NotificationConfiguration*		

Tipos de recursos definidos pelo AWS User Notifications

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}	

Chaves de condição para o AWS User Notifications

AWS As notificações do usuário definem as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para AWS User Notifications Contacts

AWS Os contatos de notificações do usuário (prefixo do serviço:`notifications-contacts`) fornecem os seguintes recursos, ações e chaves de contexto de condições específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS User Notifications Contacts
- Tipos de recursos definidos pelo AWS User Notifications Contacts
- Chaves de condição para o AWS User Notifications Contacts

Ações definidas pelo AWS User Notifications Contacts

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de

recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ActivateEmailContact	Concede permissão para ativar o contato de e-mail associado ao ARN fornecido se o código fornecido for válido	Gravar	EmailContactResource*		
CreateEmailContact	Concede permissão para criar um contato de e-mail	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteEmailContact	Concede permissão para excluir um contato de e-mail associado ao ARN fornecido	Gravar	EmailContactResource*		
GetEmailContact	Concede permissão para obter um contato de e-mail associado ao ARN fornecido	Leitura	EmailContactResource*		
ListEmailContacts	Concede permissão para listar contatos de e-mail	Lista			
ListTagsForResource	Concede permissão para obter tags para um recurso	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
SendActivationCode	Concede permissão para enviar um link de ativação para o e-mail associado ao ARN fornecido	Gravar	EmailContactResource*		
TagResource	Concede permissão para marcar um recurso	Tags	EmailContactResource*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover etiquetas de um recurso	Tags	EmailContactResource*		
				aws:TagKeys	

Tipos de recursos definidos pelo AWS User Notifications Contacts

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
EmailContactResource	`arn:${Partition}:notifications-contacts::${Account}:emailcontact/${EmailContactId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o AWS User Notifications Contacts

AWS Os contatos de notificações do usuário definem as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS User Subscriptions

AWS As assinaturas de usuário (prefixo do serviço:`user-subscriptions`) fornecem os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS User Subscriptions
- Tipos de recursos definidos pelo AWS User Subscriptions
- Chaves de condição do AWS User Subscriptions

Ações definidas pelo AWS User Subscriptions

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de

condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateClaim	Concede permissão para criar uma solicitação de assinatura de usuário	Gravar		user-subscriptions:CreateForSelf	
DeleteClaim	Concede permissão para excluir uma solicitação de assinatura de usuário	Gravar			
ListApplicationClaims	Concede permissão para listar todas as solicitações de assinatura de usuários para a aplicação	Lista			
ListClaims	Concede permissão para listar todas as solicitações de assinatura de usuários	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListUserSubscriptions	Concede permissão para listar todas as assinaturas de usuários	Lista			
UpdateClaim	Concede permissão para atualizar uma solicitação de assinatura de usuário	Gravar			

Tipos de recursos definidos pelo AWS User Subscriptions

AWS As assinaturas de usuários não oferecem suporte à especificação de um ARN de recurso no `Resource` elemento de uma declaração de política do IAM. Para permitir acesso ao AWS User Subscriptions, especifique o `"Resource": "*"` na política.

Chaves de condição do AWS User Subscriptions

AWS As assinaturas de usuário definem as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
user-subscriptions:CreateForSelf	Filtra o acesso permitindo apenas a criação de solicitações de assinatura de usuário para o chamador	Bool

Ações, recursos e chaves de condição para o AWS Verified Access

AWS O Acesso Verificado (prefixo do serviço:`verified-access`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Verified Access
- Tipos de recursos definidos pelo AWS Verified Access
- Chaves de condição do AWS Verified Access

Ações definidas pelo AWS Verified Access

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar

a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AllowVerifiedAccess [somente permissão]	Concede permissão para criar uma instância do Verified Access	Gravar			

Tipos de recursos definidos pelo AWS Verified Access

AWS O acesso verificado não é compatível com a especificação de um ARN de recurso `Resource` no elemento de uma declaração de política do IAM. Para conceder acesso ao AWS Verified Access, especifique `"Resource": "*"` na política.

Chaves de condição do AWS Verified Access

O Verified Access não tem chaves de contexto específicas ao serviço que possam ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição do Amazon Verified Permissions

O Amazon Verified Permissions (prefixo de serviço: `verifiedpermissions`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon Verified Permissions
- Tipos de recursos definidos pelo Amazon Verified Permissions
- Chaves de condição para o Amazon Verified Permissions

Ações definidas pelo Amazon Verified Permissions

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateIdentitySource	Concede permissão para criar uma referência a um provedor de identidades (IdP) externo compatível com protocolo de autenticação OpenID Connect	Gravar	policy-store*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	(OIDC), como o Amazon Cognito				
CreatePolicy	Concede permissão para criar uma política do Cedar e salvá-la no repositório de políticas especificado	Gravar	policy-store*		
CreatePolicyStore	Concede permissão para criar uma política do Cedar e salvá-la no repositório de políticas especificado	Gravar		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreatePolicyTemplate	Concede permissão para criar um modelo de política	Gravar	policy-store*		
DeleteIdentitySource	Concede permissão para excluir uma fonte de identidade que faz referência a um provedor de identidade (IdP) como o Amazon Cognito	Gravar	policy-store*		
DeletePolicy	Concede permissão para excluir a política especificada do repositório de políticas	Gravar	policy-store*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeletePolicyStore	Concede permissão para excluir o repositório de políticas especificado	Gravar	policy-store*		
DeletePolicyTemplate	Concede permissão para excluir o modelo de política especificada do repositório de políticas	Gravar	policy-store*		
GetIdentitySource	Concede permissão para recuperar os detalhes sobre a fonte de identidade especificada	Leitura	policy-store*		
GetPolicy	Concede permissão para recuperar informações sobre a política especificada	Leitura	policy-store*		
GetPolicyStore	Concede permissão para recuperar detalhes sobre um repositório de políticas	Leitura	policy-store*		verifiedpermissions:ListTagsForResource
GetPolicyTemplate	Concede permissão para recuperar os detalhes do modelo de política especificada do repositório de políticas especificado	Leitura	policy-store*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSchema	Concede permissão para recuperar os detalhes do esquema especificado do repositório de políticas especificado	Leitura	policy-store*		
IsAuthorized	Concede permissão para tomar uma decisão de autorização sobre uma solicitação de serviço descrita nos parâmetros	Leitura	policy-store*		
IsAuthorizedWithToken	Concede permissão para tomar uma decisão de autorização sobre uma solicitação de serviço descrita nos parâmetros. A entidade principal nessa solicitação vem de uma fonte de identidade externa	Leitura	policy-store*		
ListIdentitySources	Concede permissão para retornar uma lista paginada de todas fontes de identidade definidas no repositório de identidade especificado	Lista	policy-store*		
ListPolicies	Concede permissão para retornar uma lista paginada de todas políticas armazenadas no repositório de políticas especificado	Lista	policy-store*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListPolicyStores	Concede permissão para retornar uma lista paginada de todos repositórios de políticas na conta de chamada da Amazon Web Services	Lista			
ListPolicyTemplates	Concede permissão para retornar uma lista paginada de todos modelos de política no repositório de políticas especificado	Lista	policy-store*		
ListTagsForResource	Concede permissão para visualizar uma lista de tags de recursos para o repositório de políticas especificado	Leitura	policy-store*		
PutSchema	Concede permissão para criar ou atualizar o esquema de política no repositório de políticas especificado	Gravar	policy-store*		
TagResource	Concede permissão para adicionar tags ao repositório de políticas especificado	Tags	policy-store*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para remover tags do repositório de políticas especificado	Tags	policy-store*		
				aws:TagKeys	
UpdateIdentitySource	Concede permissão para atualizar a fonte de identidade especificada para usar uma nova fonte de provedor de identidade (IdP) ou para alterar o mapeamento de identidades do IdP para um tipo de entidade principal diferente	Gravar	policy-store*		
UpdatePolicy	Concede permissão para modificar a política estática do Cedar especificada no repositório de políticas especificado	Gravar	policy-store*		
UpdatePolicyStore	Concede permissão para modificar a configuração de validação de um repositório de políticas	Gravar	policy-store*		
UpdatePolicyTemplate	Concede permissão para atualizar o modelo de política especificado	Gravar	policy-store*		

Tipos de recursos definidos pelo Amazon Verified Permissions

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
policy-store	`arn:${Partition}:verifiedpermissions::${Account}:policy-store/${PolicyStoreId}`	aws:ResourceTag/${TagKey}

Chaves de condição para o Amazon Verified Permissions

As permissões verificadas da Amazon definem as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por um par de chave valor da etiqueta que é permitido na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso por um par de chave e valor da etiqueta de um recurso.	Segmento

Chaves de condição	Descrição	Tipo
aws:TagKeys	Filtra o acesso por uma lista de chaves da etiqueta que são permitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do Amazon VPC Lattice

O Amazon VPC Lattice (prefixo do serviço: `vpc-lattice`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon VPC Lattice
- Tipos de recursos definidos pelo Amazon VPC Lattice
- Chaves de condição do Amazon VPC Lattice

Ações definidas pelo Amazon VPC Lattice

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
Associate ViaAWSService [somente permissão]	Concede permissão para associar uma configuração de recursos por meio de qualquer rede gerenciada por AWS serviços	Gerenciamento de permissões			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateViaAWSService-EventsAndStates [somente permissão]	Concede permissão para associar uma configuração de recurso por meio das redes de serviços Amazon EventBridge e AWS Step Functions	Gerenciamento de permissões			
CreateAccessLogSubscription	Concede permissão para criar uma assinatura de logs de acesso	Gravar	AccessLogSubscription*		logs:CreateLogDelivery logs:GetLogDelivery
			ResourceConfiguration		
			Service		
			ServiceNetwork		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateListener	Concede permissão para criar um receptor	Gravar	Listener*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:Protocol vpc-lattice:TargetGroupArns	
CreateResourceConfiguration	Concede permissão para criar uma configuração de recurso	Gravar	ResourceConfiguration		
			ResourceGateway		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateResourceGateway	Concede permissão para criar um gateway de recursos	Gravar	ResourceGateway*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:VpcId	
CreateRule	Concede permissão para criar uma regra	Gravar	Rule*		
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:TargetGroupArns	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateService	Concede permissão para criar um serviço	Gravar	Service*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:AuthType	
CreateServiceNetwork	Concede permissão para criar uma rede de serviço	Gravar	ServiceNetwork*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:AuthType	
CreateServiceNetworkResourceAssociation	Concede permissão para criar uma associação entre uma rede de serviços e um recurso	Gravar	ResourceConfiguration*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			ServiceNetwork*		
			ServiceNetworkResourceAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:ResourceConfigurationArn vpc-lattice:ServiceNetworkArn	
CreateServiceNetworkServiceAssociation	Concede permissão para criar uma rede de serviço e associação de serviço	Gravar	Service*		
			ServiceNetwork*		
			ServiceNetworkServiceAssociation*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn	
CreateServiceNetworkVpcAssociation	Concede permissão para criar uma rede de serviço e associação de VPC	Gravar	ServiceNetwork*		ec2:DescribeVpcs
			ServiceNetworkVpcAssociation*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:SecurityGroupIds vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	
CreateServiceNetworkVpcEndpointAssociation [somente permissão]	Concede permissão para criar uma associação entre uma rede de serviços e um VPC endpoint	Gerenciamento de permissões			
CreateTargetGroup	Concede permissão para criar um grupo de destino	Gravar	TargetGroup*		iam:CreateServiceLinkedRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:VpcId	
DeleteAccessLogSubscription	Concede permissão para excluir uma assinatura de logs de acesso	Gravar	AccessLogSubscription*		logs:DeleteLogDelivery logs:GetLogDelivery
				aws:ResourceTag/${TagKey}	
DeleteAuthPolicy	Concede permissão para excluir uma política de autenticação	Gerenciamento de permissões	Service		
			ServiceNetwork		
DeleteListener	Concede permissão para excluir um receptor	Gravar	Listener*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteResourceConfiguration	Concede permissão para excluir uma configuração de recurso	Gravar	ResourceConfiguration*		
				aws:ResourceTag/${TagKey}	
DeleteResourceEndpointAssociation	Concede permissão para excluir uma associação de endpoint de recurso	Gravar	ResourceEndpointAssociation*		
				aws:ResourceTag/${TagKey}	
DeleteResourceGateway	Concede permissão para excluir um gateway de recursos	Gravar	ResourceGateway*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	Concede permissão para excluir uma política de recurso	Gravar	ResourceConfiguration		
			Service		
			ServiceNetwork		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteRule	Concede permissão para excluir uma regra	Gravar	Rule*		
				aws:ResourceTag/${TagKey}	
DeleteService	Concede permissão para excluir um serviço	Gravar	Service*		
				aws:ResourceTag/${TagKey}	
DeleteServiceNetwork	Concede permissão para excluir uma rede de serviço	Gravar	ServiceNetwork*		
				aws:ResourceTag/${TagKey}	
DeleteServiceNetworkResourceAssociation	Concede permissão para excluir a associação entre uma rede de serviços e um recurso	Gravar	ServiceNetworkResourceAssociation*		
				aws:ResourceTag/${TagKey}	
DeleteServiceNetworkServiceAssociation	Concede permissão para excluir uma rede de serviço e associação de serviço	Gravar	ServiceNetworkServiceAssociation*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn	
DeleteServiceNetworkVpcAssociation	Concede permissão para excluir uma rede de serviço e associação de VPC	Gravar	ServiceNetworkVpcAssociation*		
				aws:ResourceTag/${TagKey} vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	
DeleteTargetGroup	Concede permissão para excluir um grupo de destino	Gravar	TargetGroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
DeregisterTargets	Concede permissão para cancelar o registro de destinos de um grupo de destinos	Gravar	TargetGroup*		
GetAccessLogSubscription	Concede permissão para obter informações sobre uma assinatura de logs de acesso	Leitura	AccessLogSubscription*		logs:GetLogDelivery
				aws:ResourceTag/${TagKey}	
GetAuthPolicy	Concede permissão para obter informações sobre uma política de autenticação	Leitura	Service		
			ServiceNetwork		
GetListener	Concede permissão para obter informações sobre um receptor	Leitura	Listener*		
				aws:ResourceTag/${TagKey}	
GetResourceConfiguration	Concede permissão para obter informações sobre a configuração de um recurso	Leitura	ResourceConfiguration*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetResourceGateway	Concede permissão para obter informações sobre um gateway de recursos	Leitura	ResourceGateway*		
				aws:ResourceTag/${TagKey}	
GetResourcePolicy	Concede permissão para obter informações sobre uma política de recursos	Leitura	ResourceConfiguration		
			Service		
			ServiceNetwork		
GetRule	Concede permissão para obter informações sobre uma regra	Leitura	Rule*		
				aws:ResourceTag/${TagKey}	
GetService	Concede permissão para obter informações sobre um serviço	Leitura	Service*		
				aws:ResourceTag/${TagKey}	
GetServiceNetwork	Concede permissão para obter informações sobre uma rede de serviço	Leitura	ServiceNetwork*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetServiceNetworkResourceAssociation	Concede permissão para obter informações sobre uma associação entre uma rede de serviços e a configuração de recursos	Leitura	ServiceNetworkResourceAssociation*		
				aws:ResourceTag/${TagKey}	
GetServiceNetworkServiceAssociation	Concede permissão para obter informações sobre uma rede de serviço e associação de serviço	Leitura	ServiceNetworkServiceAssociation*		
				aws:ResourceTag/${TagKey} vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn	
GetServiceNetworkVpcAssociation	Concede permissão para obter informações sobre uma rede de serviço e associação de VPC	Leitura	ServiceNetworkVpcAssociation*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	
GetTargetGroup	Concede permissão para obter informações sobre um grupo de destinos	Leitura	TargetGroup*		
				aws:ResourceTag/${TagKey}	
ListAccessLogSubscriptions	Concede permissão para listar algumas ou todas as assinaturas de logs de acesso de uma rede de serviço ou um serviço	Lista			
ListListeners	Concede permissão para listar alguns ou todos os receptores	Lista			
ListResourceConfigurations	Concede permissão para listar algumas ou todas as configurações de recursos	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListResourceEndpointAssociations	Concede permissão para listar algumas ou todas as associações entre uma configuração de recurso e um VPC endpoint	Lista		vpc-lattice:ResourceConfigurationArn vpc-lattice:VpcEndpointId	
ListResourceGateways	Concede permissão para listar alguns ou todos os gateways de recursos	Lista			
ListRules	Concede permissão para listar algumas ou todas as regras	Lista			
ListServiceNetworkResourceAssociations	Concede permissão para listar algumas ou todas as associações entre uma rede de serviços e uma configuração de recursos	Lista			
ListServiceNetworkServiceAssociations	Concede permissão para listar algumas ou todas as redes de serviço e associações de serviço	Lista		vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListServiceNetworkVpcAssociations	Concede permissão para listar algumas ou todas as redes de serviço e associações de VPC	Lista		vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	
ListServiceNetworkVpcEndpointAssociations	Concede permissão para listar algumas ou todas as associações entre uma rede de serviços e um VPC endpoint	Lista			
ListServiceNetworks	Concede permissão para listar as redes de serviço de propriedade de uma conta do chamador ou compartilhadas com essa conta	Lista			
ListServices	Concede permissão para listar os serviços de propriedade de uma conta do chamador ou compartilhados com ela	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso do vpc-lattice	Leitura			
ListTargetGroups	Concede permissão para listar alguns ou todos os grupos de destinos	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListTargets	Concede permissão para listar alguns ou todos os destinos em um grupo de destinos	Lista	TargetGroup*		
PutAuthPolicy	Concede permissão para criar ou atualizar a política de autenticação de uma rede de serviço ou serviço	Gerenciamento de permissões	Service		
			ServiceNetwork		
PutResourcePolicy	Concede permissão para criar uma política de recursos para uma configuração de recursos, serviço ou rede de serviços	Gravar	ResourceConfiguration		
			Service		
			ServiceNetwork		
RegisterTargets	Concede permissão para registrar destinos em um grupo de destinos	Gravar	TargetGroup*		
TagResource	Concede permissão para etiquetar um recurso do vpc-lattice	Tags	AccessLogSubscription		
			Listener		
			ResourceConfiguration		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			ResourceEndpointAssociation		
			ResourceGateway		
			Rule		
			Service		
			ServiceNetwork		
			ServiceNetworkResourceAssociation		
			ServiceNetworkServiceAssociation		
			ServiceNetworkVpcAssociation		
			TargetGroup		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover etiquetas um recurso do vpc-lattice	Tags	AccessLogSubscription		
			Listener		
			ResourceConfiguration		
			ResourceEndpointAssociation		
			ResourceGateway		
			Rule		
			Service		
			ServiceNetwork		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			ServiceNetworkResourceAssociation		
			ServiceNetworkServiceAssociation		
			ServiceNetworkVpcAssociation		
			TargetGroup		
				aws:TagKeys	
UpdateAccessLogSubscription	Concede permissão para atualizar uma assinatura de logs de acesso	Gravar	AccessLogSubscription*		logs:GetLogDelivery logs:UpdateLogDelivery
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateListener	Concede permissão para atualizar um receptor	Gravar	Listener*		
				aws:ResourceTag/${TagKey} vpc-lattice:TargetGroupArns	
UpdateResourceConfiguration	Concede permissão para atualizar a configuração de um recurso	Gravar	ResourceConfiguration*		
				aws:ResourceTag/${TagKey}	
UpdateResourceGateway	Concede permissão para atualizar um gateway de recursos	Gravar	ResourceGateway*		
				aws:ResourceTag/${TagKey} vpc-lattice:SecurityGroupIds	
UpdateRule	Concede permissão para atualizar uma regra	Gravar	Rule*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey} vpc-lattice:TargetGroupArns	
UpdateService	Concede permissão para atualizar um serviço	Gravar	Service*		
				aws:ResourceTag/${TagKey} vpc-lattice:AuthType	
UpdateServiceNetwork	Concede permissão para atualizar uma rede de serviço	Gravar	ServiceNetwork*		
				aws:ResourceTag/${TagKey} vpc-lattice:AuthType	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateServiceNetworkVpcAssociation	Concede permissão para atualizar uma rede de serviço e associação de VPC	Gravar	ServiceNetworkVpcAssociation*		ec2:DescribeSecurityGroups ec2:DescribeVpcs
				aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:SecurityGroupIds vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	
UpdateTargetGroup	Concede permissão para atualizar um grupo de destinos	Gravar	TargetGroup*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pelo Amazon VPC Lattice

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
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

Chaves de condição do Amazon VPC Lattice

O Amazon VPC Lattice define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra acesso pela presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações pela presença de chaves da etiqueta na solicitação	ArrayOfString
vpc-lattice:AuthType	Filtra o acesso pelo tipo de autenticação especificado na solicitação	String
vpc-lattice:Protocol	Filtra o acesso pelo protocolo especificado na solicitação	String
vpc-lattice:ResourceConfigurationArn	Filtra o acesso pelo ARN de uma configuração de recurso	ARN
vpc-lattice:SecurityGroupIds	Filtra o acesso por grupos IDs de segurança	ArrayOfString

Chaves de condição	Descrição	Tipo
vpc-lattice:ServiceArn	Filtra o acesso pelo ARN de um serviço	ARN
vpc-lattice:ServiceNetworkArn	Filtra o acesso pelo ARN de uma rede de serviço	ARN
vpc-lattice:TargetGroupArns	Filtra o ARNs acesso por grupos-alvo	ArrayOfARN
vpc-lattice:VpcEndpointId	Filtra o acesso pelo ID de um VPC endpoint	String
vpc-lattice:VpcId	Filtra o acesso pelo ID de uma nuvem privada virtual (VPC)	String

Ações, recursos e chaves de condição do Amazon VPC Lattice Services

O Amazon VPC Lattice Services (prefixo do serviço: `vpc-lattice-svcs`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso em políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon VPC Lattice Services
- Tipos de recursos definidos pelo Amazon VPC Lattice Services
- Chaves de condição do Amazon VPC Lattice Services

Ações definidas pelo Amazon VPC Lattice Services

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
Connect	Concede permissão para se conectar a um serviço do VPC Lattice	Gravar	TCP Service*		
				vpc-lattice-svcs:Port vpc-lattice-svcs:ServiceNetworkArn vpc-lattice-svcs:ServiceArn vpc-lattice-svcs:SourceVpc vpc-lattice-svcs:SourceVpcOwnerAccount	
Invoke	Concede permissão para invocar um serviço do VPC Lattice	Gravar	Service*		
				vpc-lattice-svcs:Port	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				vpc-lattice-svcs:ServiceNetworkArn vpc-lattice-svcs:ServiceArn vpc-lattice-svcs:SourceVpc vpc-lattice-svcs:SourceVpcOwnerAccount vpc-lattice-svcs:RequestHeader/${HeaderName} vpc-lattice-svcs:RequestQueryString/	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				${QueryStringKey}	

Tipos de recursos definidos pelo Amazon VPC Lattice Services

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
Service	`arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}/${RequestPath}`	
TCP Service	`arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}`	

Chaves de condição do Amazon VPC Lattice Services

O Amazon VPC Lattice Services define as seguintes chaves de condição que podem ser usadas no elemento `Condition` de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
vpc-lattice-svcs:Port	Filtra o acesso por porta de destino para a qual a solicitação é feita	Numérico
vpc-lattice-svcs:RequestHeader/${HeaderName}	Filtra o acesso por um par nome-valor de cabeçalho nos cabeçalhos da solicitação	String
vpc-lattice-svcs:RequestMethod	Filtra o acesso pelo método da solicitação	String
vpc-lattice-svcs:RequestQueryString/${QueryStringKey}	Filtra o acesso pelos pares de chave-valor da string de consulta no URL de solicitação	ArrayOfString
vpc-lattice-svcs:ServiceArn	Filtra o acesso pelo ARN do serviço que recebe a solicitação	ARN
vpc-lattice-svcs:ServiceNetworkArn	Filtra o acesso pelo ARN da rede de serviço que recebe a solicitação	ARN
vpc-lattice-svcs:SourceVpc	Filtra o acesso pela VPC de onde a solicitação é feita	String
vpc-lattice-svcs:SourceVpcOwnerAccount	Filtra o acesso pela conta proprietária da VPC da qual a solicitação é feita	String

Ações, recursos e chaves de condição para o AWS WAF

AWS O WAF (prefixo do serviço:`waf`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS WAF
- Tipos de recursos definidos pelo AWS WAF
- Chaves de condição do AWS WAF

Ações definidas pelo AWS WAF

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateByteMatchSet	Concede permissão para criar um ByteMatchSet	Gravar	bytematchset*		
CreateGeoMatchSet	Concede permissão para criar um GeoMatchSet	Gravar	geomatchset*		
CreateIPSet	Concede permissão para criar um IPSet	Gravar	ipset*		
CreateRateBasedRule	Concede permissão para criar um RateBasedRule para limitar o volume de solicitações de um único endereço IP	Gravar	ratebasedrule*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRegexMatchSet	Concede permissão para criar um RegexMatchSet	Gravar	regexmatchset*		
CreateRegexPatternSet	Concede permissão para criar um RegexPatternSet	Gravar	regexpatternset*		
CreateRule	Concede permissão para criar uma Rule para filtrar solicitações da Web	Gravar	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleGroup	Concede permissão para criar um RuleGroup, que é uma coleção de regras predefinidas que você pode usar em uma WebACL	Gravar	rulegroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSizeConstraintSet	Concede permissão para criar um SizeConstraintSet	Gravar	sizeconstraintset*		
CreateSqlInjectionMatchSet	Concede permissão para criar um SqlInjectionMatchSet	Gravar	sqlinjectionmatchset*		
CreateWebACL	Concede permissão para criar uma WebACL, que contém regras para filtrar solicitações da Web	Gerenciamento de permissões	webacl*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebACLMigrationStack	Concede permissão para criar um modelo de ACL CloudFormation da web em um bucket do S3 com o objetivo de migrar a ACL da web do WAF Classic para o AWS WAF v2 AWS	Gravar	webacl*		s3:PutObject
CreateXssMatchSet	Concede permissão para criar um XssMatchSet, que você usa para detectar solicitações que contêm ataques de script entre sites	Gravar	xssmatchset*		
DeleteByteMatchSet	Concede permissão para excluir um ByteMatchSet	Gravar	bytematchset*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteGeoMatchSet	Concede permissão para excluir um GeoMatchSet	Gravar	geomatchset*		
DeleteIPSet	Concede permissão para excluir um IPSet	Gravar	ipset*		
DeleteLoggingConfiguration	Concede permissão para excluir o LoggingConfiguration de uma ACL da web	Gravar	webacl*		
DeletePermissionPolicy	Concede permissão para excluir uma política do IAM de um grupo de regras	Gerenciamento de permissões	rulegroup*		
DeleteRateBasedRule	Concede permissão para excluir um RateBasedRule	Gravar	ratebasedrule*		
DeleteRegexMatchSet	Concede permissão para excluir um RegexMatchSet	Gravar	regexmatchset*		
DeleteRegexPatternSet	Concede permissão para excluir um RegexPatternSet	Gravar	regexpatternset*		
DeleteRule	Concede permissão para excluir uma Rule	Gravar	rule*		
DeleteRuleGroup	Concede permissão para excluir um RuleGroup	Gravar	rulegroup*		
DeleteSizeConstraintSet	Concede permissão para excluir um SizeConstraintSet	Gravar	sizeconstraintset*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteSqlInjectionMatchSet	Concede permissão para excluir um SqlInjectionMatchSet	Gravar	sqlinjectionmatchset*		
DeleteWebACL	Concede permissão para excluir uma WebACL	Gerenciamento de permissões	webacl*		
DeleteXssMatchSet	Concede permissão para excluir um XssMatchSet	Gravar	xssmatchset*		
GetByteMatchSet	Concede permissão para recuperar um ByteMatchSet	Leitura	bytematchset*		
GetChangeToken	Concede permissão para recuperar um token de alteração para usar em solicitações de criação, atualização e exclusão	Read			
GetChangeTokenStatus	Concede permissão para recuperar o status de um token de alteração	Leitura			
GetGeoMatchSet	Concede permissão para recuperar um GeoMatchSet	Leitura	geomatchset*		
GetIPSet	Concede permissão para recuperar um IPSet	Leitura	ipset*		
GetLoggingConfiguration	Concede permissão para recuperar uma LoggingConfiguration ACL para uma web	Leitura	webacl*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetPermissionPolicy	Concede permissão para recuperar uma política do IAM para um grupo de regras	Leitura	rulegroup*		
GetRateBasedRule	Concede permissão para recuperar um RateBasedRule	Leitura	ratebasedrule*		
GetRateBasedRuleManagedKeys	Concede permissão para recuperar a matriz de endereços IP que estão atualmente sendo bloqueados por um RateBasedRule	Leitura	ratebasedrule*		
GetRegexMatchSet	Concede permissão para recuperar um RegexMatchSet	Leitura	regexmatchset*		
GetRegexPatternSet	Concede permissão para recuperar um RegexPatternSet	Leitura	regexpatternset*		
GetRule	Concede permissão para recuperar uma Rule	Leitura	rule*		
GetRuleGroup	Concede permissão para recuperar um RuleGroup	Leitura	rulegroup*		
GetSampledRequests	Concede permissão para recuperar informações detalhadas sobre um conjunto de exemplos de solicitações da Web	Leitura	webacl		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSizeConstraintSet	Concede permissão para recuperar um SizeConstraintSet	Leitura	sizeconstraintset*		
GetSqlInjectionMatchSet	Concede permissão para recuperar um SqlInjectionMatchSet	Leitura	sqlinjectionmatchset*		
GetWebACL	Concede permissão para recuperar uma WebACL	Leitura	webacl*		
GetXssMatchSet	Concede permissão para recuperar um XssMatchSet	Leitura	xssmatchset*		
ListActivatedRulesInRuleGroup	Concede permissão para recuperar uma matriz de objetos ActivatedRule	Lista			
ListByteMatchSets	Concede permissão para recuperar uma matriz de objetos ByteMatchSetSummary	Lista			
ListGeoMatchSets	Concede permissão para recuperar uma matriz de objetos GeoMatchSetSummary	Lista			
ListIPSets	Concede permissão para recuperar uma matriz de objetos IPSet Summary	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListLoggingConfigurations	Concede permissão para recuperar uma matriz de objetos LoggingConfiguration	Lista			
ListRateBasedRules	Concede permissão para recuperar uma matriz de objetos RuleSummary	Lista			
ListRegexMatchSets	Concede permissão para recuperar uma matriz de objetos RegexMatchSetSummary	Lista			
ListRegexPatternSets	Concede permissão para recuperar uma matriz de objetos RegexPatternSetSummary	Lista			
ListRuleGroups	Concede permissão para recuperar uma matriz de objetos RuleGroup	Lista			
ListRules	Concede permissão para recuperar uma matriz de objetos RuleSummary	Lista			
ListSizeConstraintSets	Concede permissão para recuperar uma matriz de objetos SizeConstraintSetSummary	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListSqlInjectionMatchSets	Concede permissão para recuperar uma matriz de objetos SqlInjectionMatchSet	Lista			
ListSubscribedRuleGroups	Concede permissão para recuperar uma matriz de RuleGroup objetos nos quais você está inscrito	Lista			
ListTagsForResource	Concede permissão para recuperar as etiquetas de um recurso	Leitura	ratebasedrule		
			rule		
			rulegroup		
			webacl		
ListWebACLs	Concede permissão para recuperar uma matriz de objetos da Web ACLSummary	Lista			
ListXssMatchSets	Concede permissão para recuperar uma matriz de objetos XssMatchSet	Lista			
PutLoggingConfiguration	Concede permissão para associar um a LoggingConfiguration a uma ACL da web especificada	Gravar	webacl*		iam:CreateServiceLinkedRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutPermissionPolicy	Concede permissão para anexar uma política do IAM a um grupo de regras para compartilhar o grupo de regras entre contas	Permissions management	rulegroup *		
TagResource	Concede permissão para adicionar uma Etiqueta a um recurso	Marcação	ratebasedrule		
			rule		
			rulegroup		
			webacl		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover uma Etiqueta de um recurso	Tags	ratebasedrule		
			rule		
			rulegroup		
			webacl		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateByteMatchSet	Concede permissão para inserir ou excluir ByteMatchTuple objetos em um ByteMatchSet	Gravar	bytematchset*		
UpdateGeoMatchSet	Concede permissão para inserir ou excluir GeoMatchConstraint objetos em um GeoMatchSet	Gravar	geomatchset*		
UpdateIPSet	Concede permissão para inserir ou excluir objetos do IPSet Descritor em um IPSet	Gravar	ipset*		
UpdateRateBasedRule	Concede permissão para modificar uma regra com base em taxa	Gravar	ratebasedrule*		
UpdateRegexMatchSet	Concede permissão para inserir ou excluir RegexMatchTuple objetos em um RegexMatchSet	Gravar	regexmatchset*		
UpdateRegexPatternSet	Concede permissão para inserir ou excluir RegexPatternStrings em um RegexPatternSet	Gravar	regexpatternset*		
UpdateRule	Concede permissão para modificar uma Rule	Gravar	rule*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateRuleGroup	Concede permissão para inserir ou excluir Activated Rule objetos em um RuleGroup	Gravar	rulegroup*		
UpdateSizeConstraintSet	Concede permissão para inserir ou excluir SizeConstraint objetos em um SizeConstraintSet	Gravar	sizeconstraintset*		
UpdateSqlInjectionMatchSet	Concede permissão para inserir ou excluir SqlInjectionMatchTuple objetos em um SqlInjectionMatchSet	Gravar	sqlinjectionmatchset*		
UpdateWebACL	Concede permissão para inserir ou excluir Activated Rule objetos em uma WebACL	Gerenciamento de permissões	webacl*		
UpdateXssMatchSet	Concede permissão para inserir ou excluir XssMatchTuple objetos em um XssMatchSet	Gravar	xssmatchset*		

Tipos de recursos definidos pelo AWS WAF

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves

são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
bytematchset	`arn:${Partition}:waf::${Account}:bytematchset/${Id}`	
ipset	`arn:${Partition}:waf::${Account}:ipset/${Id}`	
ratebasedrule	`arn:${Partition}:waf::${Account}:ratebasedrule/${Id}`	aws:ResourceTag/${TagKey}
rule	`arn:${Partition}:waf::${Account}:rule/${Id}`	aws:ResourceTag/${TagKey}
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}`	

Tipos de recursos	ARN	Chaves de condição
rulegroup	`arn:${Partition}:waf::${Account}:rulegroup/${Id}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS WAF

AWS O WAF define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base no conjunto de valores permitidos para cada uma das etiquetas	String
aws:ResourceTag/${TagKey}	Filtra ações com base no etiqueta-value associado ao recurso	String
aws:TagKeys	Filtra ações com base na presença de etiquetas obrigatórias na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS WAF Regional

AWS O WAF Regional (prefixo do serviço:`waf-regional`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.

- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS WAF Regional
- Tipos de recursos definidos pelo AWS WAF Regional
- Chaves de condição do AWS WAF Regional

Ações definidas pelo AWS WAF Regional

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateWebACL	Concede permissão para associar uma Web ACL a um recurso.	Gravar	loadbalancer/app/*		
			webacl*		
CreateByteMatchSet	Concede permissão para criar um ByteMatchSet	Gravar	bytematchset*		
CreateGeoMatchSet	Concede permissão para criar um GeoMatchSet	Gravar	geomatchset*		
CreateIPSet	Concede permissão para criar um IPSet	Gravar	ipset*		
CreateRateBasedRule	Concede permissão para criar um RateBasedRule	Gravar	ratebasedrule*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateRegexMatchSet	Concede permissão para criar um RegexMatchSet	Gravar	regexmatchset*		
CreateRegexPatternSet	Concede permissão para criar um RegexPatternSet	Gravar	regexpatternset*		
CreateRule	Concede permissão para criar uma Rule.	Gravar	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleGroup	Concede permissão para criar um RuleGroup	Gravar	rulegroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSizeConstraintSet	Concede permissão para criar um SizeConstraintSet	Gravar	sizeconstraintset*		
CreateSqlInjectionMatchSet	Concede permissão para criar um SqlInjectionMatchSet	Gravar	sqlinjectionmatchset*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateWebACL	Concede permissão para criar uma WebACL	Gerenciamento de permissões	webacl*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebACLMigrationStack	Concede permissão para criar um modelo de ACL CloudFormation da web em um bucket do S3 com o objetivo de migrar a ACL da web do WAF Classic para o AWS WAF v2 AWS	Gravar	webacl*		s3:PutObject
CreateXssMatchSet	Concede permissão para criar um XssMatchSet	Gravar	xssmatchset*		
DeleteByteMatchSet	Concede permissão para excluir um ByteMatchSet	Gravar	bytematchset*		
DeleteGeoMatchSet	Concede permissão para excluir um GeoMatchSet	Gravar	geomatchset*		
DeleteIPSet	Concede permissão para excluir um IPSet	Gravar	ipset*		
DeleteLoggingConfiguration	Concede permissão para excluir um LoggingConfiguration de uma ACL da web	Gravar	webacl*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeletePermissionPolicy	Concede permissão para excluir uma política do IAM de um grupo de regras	Gerenciamento de permissões	rulegroup*		
DeleteRateBasedRule	Concede permissão para excluir um RateBasedRule	Gravar	ratebasedrule*		
DeleteRegexMatchSet	Concede permissão para excluir um RegexMatchSet	Gravar	regexmatchset*		
DeleteRegexPatternSet	Concede permissão para excluir um RegexPatternSet	Gravar	regexpatternset*		
DeleteRule	Concede permissão para excluir uma Rule	Gravar	rule*		
DeleteRuleGroup	Concede permissão para excluir um RuleGroup	Gravar	rulegroup*		
DeleteSizeConstraintSet	Concede permissão para excluir um SizeConstraintSet	Gravar	sizeconstraintset*		
DeleteSqlInjectionMatchSet	Concede permissão para excluir um SqlInjectionMatchSet	Gravar	sqlinjectionmatchset*		
DeleteWebACL	Concede permissão para excluir uma WebACL	Gerenciamento de permissões	webacl*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteXssMatchSet	Concede permissão para excluir um XssMatchSet	Gravar	xssmatchset*		
DisassociateWebACL	Concede permissão para excluir uma associação entre uma ACL da Web e um recurso	Gravar	loadbalancer/app/*		
GetByteMatchSet	Concede permissão para recuperar um ByteMatchSet	Leitura	bytematchset*		
GetChangeToken	Concede permissão para recuperar um token de alteração para usar em solicitações de criação, atualização e exclusão	Read			
GetChangeTokenStatus	Concede permissão para recuperar o status de um token de alteração	Leitura			
GetGeoMatchSet	Concede permissão para recuperar um GeoMatchSet	Leitura	geomatchset*		
GetIPSet	Concede permissão para recuperar um IPSet	Leitura	ipset*		
GetLoggingConfiguration	Concede permissão para recuperar um LoggingConfiguration	Leitura	webacl*		
GetPermissionPolicy	Concede permissão para recuperar uma política do IAM anexada a um RuleGroup	Leitura	rulegroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetRateBasedRule	Concede permissão para recuperar um RateBasedRule	Leitura	ratebasedrule*		
GetRateBasedRuleManagedKeys	Concede permissão para recuperar a matriz de endereços IP que estão atualmente sendo bloqueados por um RateBasedRule	Leitura	ratebasedrule*		
GetRegexMatchSet	Concede permissão para recuperar um RegexMatchSet	Leitura	regexmatchset*		
GetRegexPatternSet	Concede permissão para recuperar um RegexPatternSet	Leitura	regexpatternset*		
GetRule	Concede permissão para recuperar uma Rule	Leitura	rule*		
GetRuleGroup	Concede permissão para recuperar um RuleGroup	Leitura	rulegroup*		
GetSampledRequests	Concede permissão para recuperar informações detalhadas para um conjunto de exemplos de solicitações da Web	Leitura	webacl		
GetSizeConstraintSet	Concede permissão para recuperar um SizeConstraintSet	Leitura	sizeconstraintset*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetSqlInjectionMatchSet	Concede permissão para recuperar um SqlInjectionMatchSet	Leitura	sqlinjectionmatchset*		
GetWebACL	Concede permissão para recuperar uma WebACL	Read	webacl*		
GetWebACLForResource	Concede permissão para recuperar uma WebACL associada a um recurso especificado	Leitura	loadbalancer/app/*		
GetXssMatchSet	Concede permissão para recuperar um XssMatchSet	Leitura	xssmatchset*		
ListActivatedRulesInRuleGroup	Concede permissão para recuperar uma matriz de objetos ActivatedRule	Lista			
ListByteMatchSets	Concede permissão para recuperar uma matriz de objetos ByteMatchSetSummary	Lista			
ListGeoMatchSets	Concede permissão para recuperar uma matriz de objetos GeoMatchSetSummary	Lista			
ListIPSets	Concede permissão para recuperar uma matriz de objetos IPSet Summary	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListLoggingConfigurations	Concede permissão para recuperar uma matriz de objetos LoggingConfiguration	Lista			
ListRateBasedRules	Concede permissão para recuperar uma matriz de objetos RuleSummary	Lista			
ListRegexMatchSets	Concede permissão para recuperar uma matriz de objetos RegexMatchSetSummary	Lista			
ListRegexPatternSets	Concede permissão para recuperar uma matriz de objetos RegexPatternSetSummary	Lista			
ListResourcesForWebACL	Concede permissão para recuperar uma matriz de recursos associados a uma WebACL especificada	Lista	webacl*		
ListRuleGroups	Concede permissão para recuperar uma matriz de objetos RuleGroup	Lista			
ListRules	Concede permissão para recuperar uma matriz de objetos RuleSummary	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListSizeConstraintSets	Concede permissão para recuperar uma matriz de objetos SizeConstraintSetSummary	Lista			
ListSqlInjectionMatchSets	Concede permissão para recuperar uma matriz de objetos SqlInjectionMatchSet	Lista			
ListSubscribedRuleGroups	Concede permissão para recuperar uma matriz de RuleGroup objetos nos quais você está inscrito	Lista			
ListTagsForResource	Concede permissão para relacionar as Etiquetas de um recurso	Leitura	ratebasedrule		
			rule		
			rulegroup		
			webacl		
ListWebACLs	Concede permissão para recuperar uma matriz de objetos da Web ACLSummary	Lista			
ListXssMatchSets	Concede permissão para recuperar uma matriz de objetos XssMatchSet	Lista			
PutLoggingConfiguration	Concede permissão para associar a a uma LoggingConfiguration ACL da web	Gravar	webacl*		iam:CreateServiceLinkedRole

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutPermissionPolicy	Concede permissão para anexar uma política do IAM a um grupo de regras especificado para oferecer suporte ao compartilhamento de grupos de regras entre contas	Permissions management	rulegroup *		
TagResource	Concede permissão para adicionar uma Etiqueta a um recurso	Marcação	ratebasedrule		
			rule		
			rulegroup		
			webacl		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover uma Etiqueta de um recurso	Tags	ratebasedrule		
			rule		
			rulegroup		
			webacl		
				aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateByteMatchSet	Concede permissão para inserir ou excluir ByteMatchTuple objetos em um ByteMatchSet	Gravar	bytematchset*		
UpdateGeoMatchSet	Concede permissão para inserir ou excluir GeoMatchConstraint objetos em um GeoMatchSet	Gravar	geomatchset*		
UpdateIPSet	Concede permissão para inserir ou excluir objetos do IPSet Descritor em um IPSet	Gravar	ipset*		
UpdateRateBasedRule	Concede permissão para inserir ou excluir objetos de predicados em uma regra baseada em taxas e atualizar os RateLimit na regra	Gravar	ratebasedrule*		
UpdateRegexMatchSet	Concede permissão para inserir ou excluir RegexMatchTuple objetos em um RegexMatchSet	Gravar	regexmatchset*		
UpdateRegexPatternSet	Concede permissão para inserir ou excluir RegexPatternStrings em um RegexPatternSet	Gravar	regexpatternset*		
UpdateRule	Concede permissão para inserir ou excluir objetos predicados em uma Rule	Gravar	rule*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateRuleGroup	Concede permissão para inserir ou excluir Activated Rule objetos em um RuleGroup	Gravar	rulegroup*		
UpdateSizeConstraintSet	Concede permissão para inserir ou excluir SizeConstraint objetos em um SizeConstraintSet	Gravar	sizeconstraintset*		
UpdateSqlInjectionMatchSet	Concede permissão para inserir ou excluir SqlInjectionMatchTuple objetos em um SqlInjectionMatchSet	Gravar	sqlinjectionmatchset*		
UpdateWebACL	Concede permissão para inserir ou excluir Activated Rule objetos em uma WebACL	Gerenciamento de permissões	webacl*		
UpdateXssMatchSet	Concede permissão para inserir ou excluir XssMatchTuple objetos em um XssMatchSet	Gravar	xssmatchset*		

Tipos de recursos definidos pelo AWS WAF Regional

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves

são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
bytematchset	`arn:${Partition}:waf-regional:${Region}:${Account}:bytematchset/${Id}`	
ipset	`arn:${Partition}:waf-regional:${Region}:${Account}:ipset/${Id}`	
loadbalancer/app/	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/app/${LoadBalancerName}/${LoadBalancerId}`	
ratebasedrule	`arn:${Partition}:waf-regional:${Region}:${Account}:ratebasedrule/${Id}`	aws:ResourceTag/${TagKey}
rule	`arn:${Partition}:waf-regional:${Region}:${Account}:rule/${Id}`	aws:ResourceTag/${TagKey}
sizeconstraintset	`arn:${Partition}:waf-regional:${Region}:${Account}:sizeconstraintset/${Id}`	
sqlinjectionmatchset	`arn:${Partition}:waf-regional:${Region}:${Account}:sqlinjectionset/${Id}`	
webacl	`arn:${Partition}:waf-regional:${Region}:${Account}:webacl/${Id}`	aws:ResourceTag/${TagKey}
xssmatchset	`arn:${Partition}:waf-regional:${Region}:${Account}:xssmatchset/${Id}`	
regexmatchset	`arn:${Partition}:waf-regional:${Region}:${Account}:regexmatch/${Id}`	

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS WAF Regional

AWS O WAF Regional define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base no conjunto de valores permitidos para cada uma das etiquetas	String
aws:ResourceTag/${TagKey}	Filtra ações com base no valor da etiqueta associada ao recurso	String
aws:TagKeys	Filtra ações com base na presença de etiquetas obrigatórias na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o AWS WAF V2

AWS O WAF V2 (prefixo do serviço:`wafv2`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS WAF V2
- Tipos de recursos definidos pelo AWS WAF V2
- Chaves de condição para o AWS WAF V2

Ações definidas pelo AWS WAF V2

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
Associate WebACL	Concede permissão para associar uma WebACL a um recurso.	Write	webacl*		amplify:AssociateWebACL apigateway:SetWebACL apprunner:AssociateWebAcl appsync:SetWebACL

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					cognito-idp:AssociateWebACL ec2:AssociateVerifiedAccessInstanceWebAcl elasticloadbalancing:SetWebAcl wafv2:GetPermissionPolicy wafv2:PutPermissionPolicy
			amplify-app		
			apigateway		
			apprunner		
			appsync		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			loadbalancer/app/		
			userpool		
			verified-access-instance		
CheckCapacity	Concede permissão para calcular os requisitos da unidade de capacidade da ACL da Web (WCU) para um escopo especificado e um conjunto de regras.	Leitura			
CreateAPIKey	Concede permissão para criar uma chave de API para uso na integração da API CAPTCHA em seus aplicativos cliente JavaScript	Gravar			
CreateIPSet	Concede permissão para criar um IPSet	Gravar	ipset*		wafv2:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRegexPatternSet	Concede permissão para criar um RegexPatternSet	Gravar	regexpatternset*		wafv2:TagResource

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleGroup	Concede permissão para criar um RuleGroup	Gravar	rulegroup*		wafv2:TagResource
			ipset		
			regexpatternset		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebACL	Concede permissão para criar uma WebACL	Gravar	webacl*		wafv2:TagResource
			ipset		
			managedruleset		
			regexpatternset		
			rulegroup		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAPIKey	Concede permissão para excluir uma chave de API	Gravar			
DeleteFirewallManagerRuleGroups	Concede permissão para excluir FirewallManagedRulesGroups de uma WebACL se não for mais gerenciada pelo Firewall Manager	Gravar	webacl*		
DeleteIPSet	Concede permissão para excluir um IPSet	Gravar	ipset*		
DeleteLoggingConfiguration	Concede permissão para excluir o LoggingConfiguration de uma WebACL	Gravar	webacl*		
				wafv2:LogScope	
DeletePermissionPolicy	Concede permissão para excluir o PermissionPolicy em um RuleGroup	Gerenciamento de permissões	rulegroup*		
DeleteRegexPatternSet	Concede permissão para excluir um RegexPatternSet	Gravar	regexpatternset*		
DeleteRuleGroup	Concede permissão para excluir um RuleGroup	Gravar	rulegroup*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteWebACL	Concede permissão para excluir uma WebACL	Gravar	webacl*		
DescribeAllManagedProducts	Concede permissão para recuperar informações de produto para um grupo de regras gerenciado	Leitura			
DescribeManagedProductsByVendor	Concede permissão para recuperar informações de produto para um grupo de regras gerenciado por um determinado fornecedor	Leitura			
DescribeManagedRuleGroup	Concede permissão para visualizar informações de alto nível para um grupo de regras gerenciado	Leitura			
DisassociateFirewallManager [somente permissão]	Concede permissão para desassociar o Firewall Manager da WebACL especificada	Gravar	webacl*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateWebACL	Concede permissão para desassociar uma WebACL de um recurso de aplicação	Gravar	amplify-app		amplify:DisassociateWebACL apigateway:SetWebACL apprunner:DisassociateWebAcl appsync:SetWebACL cognito-idp:DisassociateWebACL ec2:DisassociateVerifiedAccessInstanceWebAcl elasticloadbalancing:SetWebAcl

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					wafv2:PutPermissionPolicy
			apigateway		
			apprunner		
			appsync		
			loadbalancer/app/		
			userpool		
			verified-access-instance		
GenerateMobileSdkReleaseUrl	Concede permissão para gerar um URL de download pré-assinado para a versão especificada do SDK móvel	Leitura			
GetDecryptedAPIKey	Concede permissão para retornar sua chave de API no formato descriptografado. Use isso para verificar os domínios de token que você definiu para a chave	Leitura			
GetIPSet	Concede permissão para recuperar detalhes sobre um IPSet	Leitura	ipset*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
GetLoggingConfiguration	Concede permissão para recuperar LoggingConfiguration para uma WebACL	Leitura	webacl*		
				aws:ResourceTag/${TagKey} wafv2:LogScope	
GetManagedRuleSet	Concede permissão para recuperar detalhes sobre um ManagedRuleSet	Leitura	managedruleset*		
GetMobileSdkRelease	Concede permissão para recuperar informações para a versão do SDK móvel especificada, incluindo notas de lançamento e etiquetas	Leitura			
GetPermissionPolicy	Concede permissão para recuperar um PermissionPolicy para um RuleGroup	Leitura	rulegroup*		
GetRateBasedStatementManagedKeys	Concede permissão para recuperar as chaves atualmente bloqueadas por uma regra com base em taxa	Leitura	webacl*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetRegexPatternSet	Concede permissão para recuperar detalhes sobre um RegexPatternSet	Leitura	regexpatternset*		
				aws:ResourceTag/${TagKey}	
GetRuleGroup	Concede permissão para recuperar detalhes sobre um RuleGroup	Leitura	rulegroup*		
				aws:ResourceTag/${TagKey}	
GetSampledRequests	Concede permissão para recuperar informações detalhadas sobre uma amostragem de solicitações da Web	Read	webacl*		
GetWebACL	Concede permissão para recuperar detalhes sobre uma WebACL	Read	webacl*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetWebACLForResource	Concede permissão para recuperar A WebACL associada a um recurso	Leitura	webacl*		amplify:GetWebACLForResource apprunner:DescribeWebAclForService cognito-idp:GetWebACLForResource ec2:GetVerifiedAccessInstanceWebAcl wafv2:GetWebACL
			amplify-app		
			apigateway		
			apprunner		
			appsync		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			loadbalancer/app/		
			userpool		
			verified-access-instance		
ListAPIKeys	Concede permissão para recuperar uma lista das chaves de API que você definiu para o escopo especificado	Lista			
ListAvailableManagedRuleGroupVersions	Concede permissão para recuperar uma matriz de versões de grupo de regra gerenciados que estão disponíveis para uso	Lista			
ListAvailableManagedRuleGroups	Concede permissão para recuperar uma matriz de grupos de regra gerenciados que estão disponíveis para uso	Lista			
ListIPSets	Concede permissão para recuperar uma matriz de objetos IPSet Summary para os conjuntos de IP que você gerencia	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListLoggingConfigurations	Concede permissão para recuperar uma matriz de seus objetos LoggingConfiguration	Lista		wafv2:LogScope	
ListManagedRuleSets	Concede permissão para recuperar uma matriz de seus objetos ManagedRuleSet	Lista			
ListMobileSdkReleases	Concede permissão para recuperar uma lista das versões disponíveis para o SDK móvel e para a plataforma de dispositivo especificada	Lista			
ListRegexPatternSets	Concede permissão para recuperar uma matriz de RegexPatternSetSummary objetos para os conjuntos de padrões regex que você gerencia	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListResourcesForWebACL	Concede permissão para recuperar uma matriz dos nomes de recursos da Amazon (ARNs) para os recursos associados a uma ACL da web	Lista	webacl*		amplify:ListResourcesForWebACL apprunner:ListAssociatedServicesForWebAcl cognito-idp:ListResourcesForWebACL ec2:DescribeVerifiedAccessInstanceWebAclAssociations
			amplify-app		
			apprunner		
			userpool		
			verified-access-instance		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListRuleGroups	Concede permissão para recuperar uma matriz de RuleGroupSummary objetos para os grupos de regras que você gerencia	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	ipset		
			regexpatternset		
			rulegroup		
			webacl		
				aws:ResourceTag/${TagKey}	
ListWebACLs	Concede permissão para recuperar uma matriz de ACLSummary objetos da Web para a Web ACLs que você gerencia	Lista			
PutFirewallManagerRuleGroups [somente permissão]	Concede permissão para criar FirewallManagedRulesGroups em uma WebACL	Gravar	webacl*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutLoggingConfiguration	Concede permissão para habilitar um LoggingConfiguration, para iniciar o registro em uma ACL da web	Gravar	webacl*		iam:CreateServiceLinkedRole
				wafv2:LogScope wafv2:LogDestinationResource	
PutManagedRuleSetVersions	Concede permissão para habilitar, criar uma nova versão ou atualizar uma versão existente de um ManagedRuleSet	Gravar	managedruleset*		
			rulegroup*		
PutPermissionPolicy	Concede permissão para anexar uma política do IAM a um recurso, usado para compartilhar grupos de regras entre contas	Gerenciamento de permissões	rulegroup*		
TagResource	Concede permissão para associar tags a um AWS recurso	Tags	ipset		
			regexpatternset		
			rulegroup		
			webacl		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permissão para desassociar tags de um recurso AWS	Tags	ipset		
			regexpatternset		
			rulegroup		
			webacl		
				aws:TagKeys	
UpdateIPSet	Concede permissão para atualizar um IPSet	Gravar	ipset*		
				aws:ResourceTag/${TagKey}	
UpdateManagedRuleSetVersionExpiryDate	Concede permissão para atualizar a data de expiração de uma versão no ManagedRuleSet	Gravar	managedruleset*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateRegexPatternSet	Concede permissão para atualizar um RegexPatternSet	Gravar	regexpatternset*		
				aws:ResourceTag/${TagKey}	
UpdateRuleGroup	Concede permissão para atualizar um RuleGroup	Gravar	rulegroup*		
			ipset		
			regexpatternset		
				aws:ResourceTag/${TagKey}	
UpdateWebACL	Concede permissão para atualizar uma WebACL	Gravar	webacl*		
			ipset		
			managedruleset		
			regexpatternset		
			rulegroup		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pelo AWS WAF V2

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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 recursos	ARN	Chaves de condição
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}`	

Chaves de condição para o AWS WAF V2

AWS O WAF V2 define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelo conjunto de valores permitido para cada uma das etiquetas	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelo valor-etiqueta associado ao recurso	String
aws:TagKeys	Filtra o acesso pela presença de etiquetas obrigatórias na solicitação	ArrayOfString
wafv2:LogDestinationResource	Filtra o acesso por ARN de destino do log para API PutLoggingConfiguration	ARN
wafv2:LogScope	Filtra o acesso por escopo de log para a API Logging Configuration	String

Ações, recursos e chaves de condição do AWS Well-Architected Tool

AWS A Well-Architected Tool (prefixo do serviço`wellarchitected`:) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger este serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Well-Architected Tool
- Tipos de recursos definidos pelo AWS Well-Architected Tool
- Chaves de condição do AWS Well-Architected Tool

Ações definidas pelo AWS Well-Architected Tool

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
Associate Lenses	Concede permissão para associar uma lente à workload especificada	Gravar	workload*		
				aws:ResourceTag/${TagKey}	
Associate Profiles	Concede permissão para associar um perfil à workload especificada	Gravar	workload*		
				aws:ResourceTag/${TagKey}	
Configure Integration [somente permissão]	Concede permissão para configurar a integração	Gravar			
CreateLensShare	Concede permissão ao proprietário de uma lente para compartilhar com outras AWS contas e usuários do IAM	Gravar	lens*		
				aws:ResourceTag/${TagKey}	
CreateLensVersion	Concede permissão para criar uma nova versão de lentes	Gravar	lens*		
				aws:ResourceTag/${TagKey}	
CreateMilestone	Concede permissão para criar um novo marco para a workload especificada	Gravar	workload*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
CreateProfile	Concede permissão para criar um novo perfil	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfileShare	Concede permissão a um proprietário de um perfil para compartilhar com outras AWS contas e usuários do IAM	Gravar	profile*		
				aws:ResourceTag/${TagKey}	
CreateReviewTemplate	Concede permissão para criar um novo modelo de revisão	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTemplateShare	Concede permissão ao proprietário de um modelo de avaliação para compartilhar com outras AWS contas e usuários do IAM	Gravar	review-template*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateWorkload	Concede permissão para criar uma nova workload	Write		aws:RequestTag/${TagKey} aws:TagKeys wellarchitected:JiraProjectKey	
CreateWorkloadShare	Concede permissão para compartilhar uma workload com outra conta	Gravar	workload*		
				aws:ResourceTag/${TagKey}	
DeleteLens	Concede permissão para excluir uma lente	Gravar	lens*		
				aws:ResourceTag/${TagKey}	
DeleteLensShare	Concede permissão para excluir um compartilhamento de lentes existente	Gravar	lens*		
				aws:ResourceTag/${TagKey}	
DeleteProfile	Concede permissão para excluir um perfil	Gravar	profile*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
DeleteProfileShare	Concede permissão para excluir um compartilhamento de perfil existente	Gravar	profile*		
				aws:ResourceTag/${TagKey}	
DeleteReviewTemplate	Concede permissão para excluir um modelo de revisão existente	Gravar	review-template*		
				aws:ResourceTag/${TagKey}	
DeleteTemplateShare	Concede permissão para excluir um compartilhamento de modelo de revisão existente	Gravar	review-template*		
				aws:ResourceTag/${TagKey}	
DeleteWorkload	Concede permissão para excluir uma workload existente	Write	workload*		
				aws:ResourceTag/${TagKey}	
DeleteWorkloadShare	Concede permissão para excluir um compartilhamento de workload existente	Write	workload*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
DisassociateLenses	Concede permissão para desassociar uma lente da workload especificada	Gravar	workload*		
				aws:ResourceTag/${TagKey}	
DisassociateProfiles	Concede permissão para desassociar um perfil da workload especificada	Gravar	workload*		
				aws:ResourceTag/${TagKey}	
ExportLens	Concede permissão para exportar uma lente existente	Leitura	lens*		
				aws:ResourceTag/${TagKey}	
GetAnswer	Concede permissão para recuperar a resposta especificada da revisão de lente especificada	Leitura	workload*		
				aws:ResourceTag/${TagKey}	
GetConsolidatedReport	Concede permissão para obter métricas de relatórios consolidados ou gerar o relatório consolidado em PDF na conta	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetGlobalSettings	Concede permissão para obter todas as configurações da conta	Leitura			
GetLens	Concede permissão para obter uma lente existente	Leitura	lens*		
				aws:ResourceTag/${TagKey}	
GetLensReview	Concede permissão para recuperar a revisão de lente especificada da workload especificada	Read	workload*		
				aws:ResourceTag/${TagKey}	
GetLensReviewReport	Concede permissão para recuperar o relatório para a revisão de lente especificada	Read	workload*		
				aws:ResourceTag/${TagKey}	
GetLensVersionDifference	Concede permissão para obter a diferença entre a versão especificada da lente e a versão mais recente da lente disponível	Read	lens*		
				aws:ResourceTag/${TagKey}	
GetMilestone	Concede permissão para recuperar o marco especificado da workload especificada	Leitura	workload*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetProfile	Concede permissão para recuperar o perfil especificado	Leitura	profile*		
				aws:ResourceTag/${TagKey}	
GetProfileTemplate	Concede permissão para recuperar o modelo de perfil especificado	Leitura			
GetReviewTemplate	Concede permissão para recuperar o modelo de revisão especificado	Leitura	review-template*		
				aws:ResourceTag/${TagKey}	
GetReviewTemplateAnswer	Concede permissão para recuperar a resposta especificada da revisão de lente do modelo de revisão especificado	Leitura	review-template*		
				aws:ResourceTag/${TagKey}	
GetReviewTemplateLensReview	Concede permissão para recuperar a revisão de lente especificada do modelo de revisão especificado	Leitura	review-template*		
				aws:ResourceTag/${TagKey}	
GetWorkload	Concede permissão para recuperar a workload especificada	Leitura	workload*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
ImportLens	Concede permissão para importar novas lentes	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
ListAnswers	Concede permissão para listar as respostas da revisão de lente especificada	Lista	workload*		
				aws:ResourceTag/${TagKey}	
ListCheckDetails	Concede permissão para listar os detalhes de verificação da workload	Lista	workload*		
				aws:ResourceTag/${TagKey}	
ListCheckSummaries	Concede permissão para listar os resumos de verificação da workload	Lista	workload*		
				aws:ResourceTag/${TagKey}	
ListLensReviewImprovements	Concede permissão para listar as melhorias da revisão de lente especificada	List	workload*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListLensReviews	Concede permissão para listar as revisões de lente da workload especificada	Lista	workload*		
				aws:ResourceTag/${TagKey}	
ListLensShares	Concede permissão para listar todos os compartilhamentos criados para uma lente	Lista	lens*		
				aws:ResourceTag/${TagKey}	
ListLenses	Concede permissão para listar as lentes disponíveis para esta conta	List			
ListMilestones	Concede permissão para listar os marcos da workload especificada	List	workload*		
				aws:ResourceTag/${TagKey}	
ListNotifications	Concede permissão para listar notificações relacionadas à conta ou ao recurso especificado	Lista			
ListProfileNotifications	Concede permissão para listar notificações de perfil relacionadas ao recurso especificado	Lista			
ListProfileShares	Concede permissão para listar todos os compartilhamentos criados para um perfil	Lista	profile*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
ListProfiles	Concede permissão para listar os perfis disponíveis para esta conta	Lista			
ListReviewTemplateAnswers	Concede permissão para listar as respostas da revisão de lente do modelo de revisão especificado	Lista	review-template*		
				aws:ResourceTag/${TagKey}	
ListReviewTemplates	Concede permissão para listar os modelos de revisão disponíveis para essa conta	Lista			
ListShareInvitations	Concede permissão para listar os convites de compartilhamento de workload da conta ou usuário especificado	List			
ListTagsForResource	Concede permissão para listar etiquetas para um recurso Well-Architected	Leitura	lens		
			profile		
			review-template		
			workload		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
ListTemplateShares	Concede permissão para listar todos os compartilhamentos criados para um modelo de revisão	Lista	review-template*		
				aws:ResourceTag/${TagKey}	
ListWorkloadShares	Concede permissão para listar os compartilhamentos de workload da workload especificada	List	workload*		
				aws:ResourceTag/${TagKey}	
ListWorkloads	Concede permissão para listar as cargas de trabalho nesta conta	List			
TagResource	Concede permissão para marcar um recurso Well-Architected	Marcação	lens		
			profile		
			review-template		
			workload		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para desmarcar um recurso Well-Architected	Marcação	lens		
			profile		
			review-template		
			workload		
				aws:TagKeys	
UpdateAnswer	Concede permissão para atualizar propriedades da resposta especificada	Gravar	workload*		
				aws:ResourceTag/${TagKey}	
UpdateGlobalSettings	Concede permissão para gerenciar todas as configurações da conta	Gravar		wellarchitected:JiraProjectKey	
UpdateIntegration	Concede permissão para atualizar as propriedades da integração	Gravar	workload*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
UpdateLensReview	Concede permissão para atualizar as propriedades da revisão de lente especificada	Gravar	workload*		
				aws:ResourceTag/${TagKey}	
UpdateProfile	Concede permissão para atualizar propriedades do perfil especificado	Gravar	profile*		
				aws:ResourceTag/${TagKey}	
UpdateReviewTemplate	Concede permissão para atualizar as propriedades do modelo de revisão especificado	Gravar	review-template*		
				aws:ResourceTag/${TagKey}	
UpdateReviewTemplateAnswer	Concede permissão para atualizar as propriedades da resposta do modelo de revisão especificado	Gravar	review-template*		
				aws:ResourceTag/${TagKey}	
UpdateReviewTemplateLensReview	Concede permissão para atualizar as propriedades da revisão de lente do modelo de revisão especificado	Gravar	review-template*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
UpdateShareInvitation	Concede permissão para atualizar o status do convite de compartilhamento de workload especificado	Write			
UpdateWorkload	Concede permissão para atualizar propriedades da workload especificada	Gravar	workload*		
				aws:ResourceTag/${TagKey} wellarchitected:JiraProjectKey	
UpdateWorkloadShare	Concede permissão para atualizar propriedades do compartilhamento de workload especificado	Gravar	workload*		
				aws:ResourceTag/${TagKey}	
UpgradeLensReview	Concede permissão para atualizar a revisão de lente especificada para usar a versão mais recente da lente associada	Gravar	workload*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpgradeProfileVersion	Concede permissão para atualizar a workload especificada para usar a versão mais recente do perfil associado	Gravar	profile*		
			workload*		
				aws:ResourceTag/${TagKey}	
UpgradeReviewTemplateLensReview	Concede permissão para atualizar a revisão de lente especificada do modelo de revisão especificado	Gravar	review-template*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pelo AWS Well-Architected Tool

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
workload	`arn:${Partition}:wellarchitected:${Region}:${Account}:workload/${ResourceId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS Well-Architected Tool

AWS A Well-Architected Tool define as seguintes chaves de condição que podem ser usadas no elemento de uma `Condition` política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso por pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta na solicitação	ArrayOfString

Chaves de condição	Descrição	Tipo
wellarchitected:JiraProjectKey	Filtra o acesso pela chave do projeto	String

Ações, recursos e chaves de condição para o AWS Wickr

AWS O Wickr (prefixo do serviço:`wickr`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS Wickr
- Tipos de recursos definidos pelo AWS Wickr
- Chaves de condição do AWS Wickr

Ações definidas pelo AWS Wickr

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateAdminSession	Concede permissão para criar e gerenciar redes do Wickr	Gravar	network*		
CreateNetwork	Concede permissão para criar uma nova rede Wickr	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteNetwork	Concede permissão para criar e excluir redes do Wickr	Gravar			
ListNetworks	Concede permissão para exibir redes do Wickr	Gravar			
ListTagsForResource	Concede permissão para listar as etiquetas aplicadas a um recurso do Wickr	Leitura			
TagResource	Concede permissão para adicionar etiquetas ao recurso do Wickr especificado	Tags	network*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permissão para desmarcar as etiquetas especificadas do recurso especificado do Wickr	Tags	network*		
				aws:TagKeys	
UpdateNetworkDetails	Concede permissão para atualizar detalhes de uma rede Wickr	Gravar	network*		

Tipos de recursos definidos pelo AWS Wickr

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
network	`arn:${Partition}:wickr:${Region}:${Account}:network/${NetworkId}`	aws:ResourceTag/${TagKey}

Chaves de condição do AWS Wickr

AWS O Wickr define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra o acesso pela chave e valor de uma etiqueta em uma solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta em uma solicitação	ArrayOfString

Ações, recursos e chaves de condição para a Amazon WorkDocs

A Amazon WorkDocs (prefixo do serviço:`workdocs`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon WorkDocs
- Tipos de recursos definidos pela Amazon WorkDocs
- Chaves de condição para Amazon WorkDocs

Ações definidas pela Amazon WorkDocs

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*).

Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AbortDocumentVersionUpload	Concede permissão para abortar o upload da versão especificada do documento que foi iniciada anteriormente pelo InitiateDocumentVersionUpload	Gravar			
ActivateUser	Concede permissão para ativar o usuário especificado. Somente usuários ativos podem acessar a Amazon WorkDocs	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AddNotificationPermissions [somente permissão]	Concede permissão para adicionar diretores que têm permissão para chamar a assinatura de notificação APIs para um determinado site WorkDocs	Gravar			
AddResourcePermissions	Concede permissão para criar um conjunto de permissões para a pasta ou documento especificado	Gravar			
AddUserToGroup [somente permissão]	Concede permissão para adicionar um usuário a um grupo	Gravar			
CheckAlias [somente permissão]	Concede permissão para verificar um alias	Leitura			
CreateComment	Concede permissão para adicionar um novo comentário à versão do documento especificada	Gravar			
CreateCustomMetadata	Concede permissão para adicionar uma ou mais propriedades personalizadas ao recurso especificado	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateFolder	Concede permissão para criar uma pasta com o nome e a pasta pai especificados	Gravar			
CreateInstance [somente permissão]	Concede permissão para criar uma instância	Gravar			
CreateLabels	Concede permissão para adicionar rótulos ao recurso especificado	Gravar			
CreateNotificationSubscription	Concede permissão para configurar e WorkDocs usar as notificações do Amazon SNS	Gravar			
CreateUser	Concede permissão para criar um usuário em um diretório do Simple AD ou do Microsoft AD	Gravar			
DeactivateUser	Concede permissão para desativar o usuário especificado, o que revoga o acesso do usuário à Amazon WorkDocs	Gravar			
DeleteComment	Concede permissão para excluir o comentário especificado da versão do documento	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteCustomMetadata	Concede permissão para excluir metadados personalizados do recurso especificado	Gravar			
DeleteDocument	Concede permissão para excluir permanentemente o documento especificado e os metadados associados	Gravar			
DeleteDocumentVersion	Concede permissão para excluir as versões de um documento especificado	Gravar			
DeleteFolder	Concede permissão para excluir permanentemente a pasta especificada e seu conteúdo	Gravar			
DeleteFolderContents	Concede permissão para excluir o conteúdo da pasta especificada	Gravar			
DeleteInstance [somente permissão]	Concede permissão para excluir uma instância	Gravar			
DeleteLabels	Concede permissão para excluir um ou mais rótulos de um recurso	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteNotification Permissions [somente permissão]	Concede permissão para excluir os diretores que têm permissão para chamar a assinatura APIs de notificação de um determinado site WorkDocs	Gravar			
DeleteNotification Subscription	Concede permissão para excluir a assinatura especificada da organização especificada	Gravar			
DeleteUser	Concede permissão para excluir o usuário especificado de um diretório do Simple AD ou do Microsoft AD	Gravar			
DeregisterDirectory [somente permissão]	Concede permissão para cancelar o registro de um diretório	Gravar			
DescribeActivities	Concede permissão para buscar atividades do usuário em um período especificado	Lista			
DescribeAvailableDirectories [somente permissão]	Concede permissão para descrever os diretórios disponíveis	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeComments	Concede permissão para listar todos os comentários da versão do documento especificada	Lista			
DescribeDocumentVersions	Concede permissão para recuperar as versões do documento especificado	Lista			
DescribeFolderContents	Concede permissão para descrever o conteúdo da pasta especificada incluindo seus documentos e subpastas	Lista			
DescribeGroups	Concede permissão para descrever os grupos de usuários	Lista			
DescribeInstanceExports [somente permissão]	Concede permissão para descrever o histórico de exportação de uma instância	Lista			
DescribeInstances [somente permissão]	Concede permissão para descrever as instâncias	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeNotificationPermissions [somente permissão]	Concede permissão para descrever os diretores que têm permissão para chamar a assinatura de notificação APIs para um determinado site WorkDocs	Lista			
DescribeNotificationSubscriptions	Concede permissão para listar as assinaturas de notificação especificadas	Lista			
DescribeResourcePermissions	Concede permissão para visualizar uma descrição das permissões de um recurso especificado	Lista			
DescribeRootFolders	Concede permissão para descrever as pastas raiz	Lista			
DescribeUsers	Concede permissão para visualizar uma descrição dos usuários especificados. Você pode descrever todos os usuários ou filtrar os resultados (por exemplo, por status ou organização)	Lista			
DownloadDocumentVersion [somente permissão]	Concede permissão para fazer download de uma versão do documento especificada	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetCurrentUser	Concede permissão para recuperar os detalhes do usuário atual	Leitura			
GetDocument	Concede permissão para recuperar o objeto de documento especificado	Leitura			
GetDocumentPath	Concede permissão para recuperar as informações de caminho (a hierarquia da pasta raiz) do documento solicitado	Leitura			
GetDocumentVersion	Concede permissão para recuperar os metadados da versão do documento especificado	Leitura			
GetFolder	Concede permissão para recuperar os metadados da pasta especificada	Leitura			
GetFolderPath	Concede permissão para recuperar as informações de caminho (a hierarquia da pasta raiz) da pasta solicitada	Leitura			
GetGroup [somente permissão]	Concede permissão para recuperar os detalhes do grupo especificado	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetResources	Concede permissão para obter uma coleção de recursos	Leitura			
InitiateDocumentVersionUpload	Concede permissão para criar um novo objeto de documento e o objeto de versão	Gravar			
RegisterDirectory [somente permissão]	Concede permissão para registrar um diretório	Gravar			
RemoveAllResourcePermissions	Concede permissão para remover todas as permissões do recurso especificado	Gravar			
RemoveResourcePermission	Concede permissão para remover a permissão da entidade principal especificada do recurso especificado	Gravar			
RestoreDocumentVersions	Concede permissão para restaurar as versões de um documento especificado	Gravar			
SearchResources	Concede permissão para pesquisar metadados e o conteúdo de recursos	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartInstanceExport [somente permissão]	Concede permissão para iniciar uma exportação de uma instância	Gravar	organization*		
UpdateDocument	Concede permissão para atualizar os atributos especificados do documento especificado	Gravar			
UpdateDocumentVersion	Concede permissão para alterar o status da versão do documento para ACTIVE (ATIVO)	Gravar			
UpdateFolder	Concede permissão para atualizar os atributos especificados da pasta especificada	Gravar			
UpdateInstanceAlias [somente permissão]	Concede permissão para atualizar um alias de instância	Gravar			
UpdateUser	Concede permissão para atualizar os atributos especificados do usuário especificado e concede ou revoga privilégios administrativos ao site da Amazon WorkDocs	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateUserAdministrativeSettings [somente permissão]	Concede permissão para atualizar as configurações administrativas para um usuário	Gravar			

Tipos de recursos definidos pela Amazon WorkDocs

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
organization	`arn:${Partition}:workdocs:${Region}:${Account}:organization/${ResourceId}`	

Chaves de condição para Amazon WorkDocs

WorkDocs não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para a Amazon WorkLink

A Amazon WorkLink (prefixo do serviço:`worklink`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon WorkLink
- Tipos de recursos definidos pela Amazon WorkLink
- Chaves de condição para Amazon WorkLink

Ações definidas pela Amazon WorkLink

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá

incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateDomain	Concede permissão para associar um domínio a uma WorkLink frota da Amazon	Gravar	fleet*		
AssociateWebsiteAuthorizationProvider	Concede permissão para associar um provedor de autorização de sites a uma WorkLink frota da Amazon	Gravar	fleet*		
AssociateWebsiteCertificateAuthority	Concede permissão para associar uma autoridade de certificação do site a uma WorkLink frota da Amazon	Gravar	fleet*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateFleet	Concede permissão para criar uma WorkLink frota da Amazon	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFleet	Concede permissão para excluir uma WorkLink frota da Amazon	Gravar	fleet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeAuditStreamConfiguration	Concede permissão para descrever a configuração do fluxo de auditoria para uma WorkLink frota da Amazon	Leitura	fleet*		
DescribeCompanyNetworkConfiguration	Concede permissão para descrever a configuração de rede da empresa para uma WorkLink frota da Amazon	Leitura	fleet*		
DescribeDevice	Concede permissão para descrever detalhes de um dispositivo associado a uma WorkLink frota da Amazon	Leitura	fleet*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeDevicePolicyConfiguration	Concede permissão para descrever a configuração da política do dispositivo para uma WorkLink frota da Amazon	Leitura	fleet*		
DescribeDomain	Concede permissão para descrever detalhes sobre um domínio associado a uma WorkLink frota da Amazon	Leitura	fleet*		
DescribeFleetMetadata	Concede permissão para descrever metadados de uma frota da Amazon WorkLink	Leitura	fleet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeIdentityProviderConfiguration	Concede permissão para descrever a configuração do provedor de identidade para uma WorkLink frota da Amazon	Leitura	fleet*		
DescribeWebsiteCertificateAuthority	Concede permissão para descrever uma autoridade de certificação do site associada a uma WorkLink frota da Amazon	Leitura	fleet*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateDomain	Concede permissão para desassociar um domínio de uma frota da Amazon WorkLink	Gravar	fleet*		
DisassociateWebsiteAuthorizationProvider	Concede permissão para desassociar um provedor de autorização de sites de uma frota da Amazon WorkLink	Gravar	fleet*		
DisassociateWebsiteCertificateAuthority	Concede permissão para desassociar uma autoridade de certificação do site de uma frota da Amazon WorkLink	Gravar	fleet*		
ListDevices	Concede permissão para listar os dispositivos associados a uma WorkLink frota da Amazon	Lista	fleet*		
ListDomains	Concede permissão para listar os domínios associados a uma frota da Amazon WorkLink	Lista	fleet*		
ListFleets	Concede permissão para listar as WorkLink frotas da Amazon associadas à conta	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura	fleet*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListWebsiteAuthorizationProviders	Concede permissão para listar os provedores de autorização do site para uma WorkLink frota da Amazon	Lista	fleet*		
ListWebsiteCertificateAuthorities	Concede permissão para listar as autoridades de certificação do site associadas a uma WorkLink frota da Amazon	Lista	fleet*		
RestoreDomainAccess	Concede permissão para restaurar o acesso a um domínio associado a uma WorkLink frota da Amazon	Gravar	fleet*		
RevokeDomainAccess	Concede permissão para revogar o acesso a um domínio associado a uma frota da Amazon WorkLink	Gravar	fleet*		
SearchEntity [somente permissão]	Concede permissão para listar dispositivos para uma WorkLink frota da Amazon	Lista	fleet*		
SignOutUser	Concede permissão para desconectar um usuário de uma WorkLink frota da Amazon	Gravar	fleet*		
TagResource	Concede permissão para adicionar uma ou mais etiquetas a um recurso	Marcação	fleet*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover uma ou mais etiquetas de um recurso	Tags	fleet*		
				aws:TagKeys	
UpdateAuditStreamConfiguration	Concede permissão para atualizar a configuração do fluxo de auditoria para uma WorkLink frota da Amazon	Gravar	fleet*		
UpdateCompanyNetworkConfiguration	Concede permissão para atualizar a configuração de rede da empresa para uma WorkLink frota da Amazon	Gravar	fleet*		
UpdateDevicePolicyConfiguration	Concede permissão para atualizar a configuração da política do dispositivo para uma WorkLink frota da Amazon	Gravar	fleet*		
UpdateDomainMetadata	Concede permissão para atualizar os metadados de um domínio associado a uma frota da Amazon WorkLink	Gravar	fleet*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateFleetMetadata	Concede permissão para atualizar os metadados de uma frota da Amazon WorkLink	Gravar	fleet*		
UpdateIdentityProviderConfiguration	Concede permissão para atualizar a configuração do provedor de identidade para uma WorkLink frota da Amazon	Gravar	fleet*		

Tipos de recursos definidos pela Amazon WorkLink

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
fleet	`arn:${Partition}:worklink::${Account}:fleet/${FleetName}`	aws:ResourceTag/${TagKey}

Chaves de condição para Amazon WorkLink

A Amazon WorkLink define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições

sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base na presença de pares de chave-valor da etiqueta na solicitação	String
aws:ResourceTag/${TagKey}	Filtra ações com base nos pares de chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra ações com base na presença de chaves da etiqueta na solicitação	ArrayOfString

Ações, recursos e chaves de condição para a Amazon WorkMail

A Amazon WorkMail (prefixo do serviço:`workmail`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon WorkMail
- Tipos de recursos definidos pela Amazon WorkMail
- Chaves de condição para Amazon WorkMail

Ações definidas pela Amazon WorkMail

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AllowVendedLogDeliveryForResource [somente permissão]	Concede permissão para configurar a entrega de registros vendidos para registros de WorkMail auditoria	Gravar	organization*		
AssociateDelegateToResource	Concede permissão para adicionar um membro (usuário ou grupo) ao conjunto de delegados do recurso.	Write	organization*		
AssociateMemberToGroup	Concede permissão para adicionar um membro (usuário ou grupo) ao conjunto do grupo.	Gravar	organization*		
AssumeImpersonationRole	Concede permissão para assumir uma função de falsificação de identidade para uma determinada organização da Amazon WorkMail	Gravar	organization*		
CancelMailboxExportJob	Concede permissão para cancelar um trabalho de exportação de caixa postal em execução no momento.	Gravar	organization*		
CreateAlias	Concede permissão para adicionar um alias ao conjunto de um determinado membro	Gravar	organization*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	(usuário ou grupo) do WorkMail				
CreateAvailability Configuration	Concede permissão para criar um AvailabilityConfiguration para a WorkMail organização e domínio da Amazon em questão	Gravar	organization*		
CreateGroup	Concede permissão para criar um grupo que pode ser usado WorkMail chamando a RegisterToWorkMail operação	Gravar	organization*		
CreateIdentityCenterApplication	Concede permissão para criar um aplicativo Identity Center para WorkMail	Gravar			
CreateImpersonationRole	Concede permissão para criar uma função de falsificação de identidade para uma determinada organização da Amazon WorkMail	Gravar	organization*		
CreateInboundMailFlowRule [somente permissão]	Concede permissão para criar uma regra de fluxo de e-mails de entrada que será aplicada a todos os e-mails enviados para uma organização.	Write	organization*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateMailDomain [somente permissão]	Concede permissão para criar um domínio de e-mail.	Gravar	organization*		
CreateMobileDeviceAccessRule	Concede permissão para criar uma regra de acesso por dispositivos móveis.	Gravar	organization*		
CreateOrganization	Concede permissão para criar uma nova WorkMail organização na Amazon	Gravar			
CreateOutboundMailFlowRule [somente permissão]	Concede permissão para criar uma regra de fluxo de e-mails de saída que será aplicada a todos os e-mails enviados de uma organização.	Gravar	organization*		
CreateResource	Concede permissão para criar um novo WorkMail recurso	Gravar	organization*		
CreateSmtpGateway [somente permissão]	Concede permissão para registrar um gateway SMTP em uma organização WorkMail	Gravar	organization*		
CreateUser	Concede permissão para criar um usuário, que pode ser ativado posteriormente chamando a RegisterToWorkMail operação	Gravar	organization*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteAccessControlRule	Concede permissão para excluir uma regra de controle de acesso.	Write	organization*		
DeleteAlias	Concede permissão para remover um ou mais aliases especificados de um conjunto de aliases de determinado usuário.	Gravar	organization*		
DeleteAvailabilityConfiguration	Concede permissão para excluir o AvailabilityConfiguration domínio e WorkMail organização da Amazon em questão	Gravar	organization*		
DeleteEmailMonitoringConfiguration	Concede permissão para excluir a configuração de monitoramento de e-mail de uma organização	Gravar	organization*		
DeleteGroup	Concede permissão para excluir um grupo de WorkMail	Gravar	organization*		
DeleteIdentityCenterApplication	Concede permissão para excluir um aplicativo do Identity Center para WorkMail	Gravar			
DeleteIdentityProviderConfiguration	Concede permissão para excluir a configuração do provedor de identidade para a organização	Gravar	organization*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteImpersonationRole	Concede permissão para excluir uma função de falsificação de identidade para uma determinada organização da Amazon WorkMail	Gravar	organization*		
DeleteInboundMailFlowRule [somente permissão]	Concede permissão para remover uma regra de fluxo de e-mails de entrada para que ela não seja mais aplicada aos e-mails enviados a uma organização.	Write	organization*		
DeleteMailDomain [somente permissão]	Concede permissão para remover um domínio de e-mail não utilizado de uma organização.	Write	organization*		
DeleteMailboxPermissions	Concede permissão para excluir permissões concedidas a um membro (usuário ou grupo).	Write	organization*		
DeleteMobileDevice [somente permissão]	Concede permissão para remover um dispositivo móvel de um usuário.	Gravar	organization*		
DeleteMobileDeviceAccessOverride	Concede permissão para excluir uma sobreposição de acesso de dispositivo móvel	Gravar	organization*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteMobileDeviceAccessRule	Concede permissão para excluir uma regra de acesso de dispositivo móvel	Gravar	organization*		
DeleteOrganization	Concede permissão para excluir uma WorkMail organização da Amazon e todos os AWS recursos subjacentes gerenciados pela Amazon WorkMail como parte da organização	Gravar	organization*		
DeleteOutboundMailFlowRule [somente permissão]	Concede permissão para remover uma regra de fluxo de e-mails de saída para que ela não se aplique mais a e-mails enviados de uma organização.	Gravar	organization*		
DeletePersonalAccessToken	Concede permissão para excluir um token de acesso pessoal	Gravar	organization*		
DeleteResource	Concede permissão para excluir o recurso especificado.	Write	organization*		
DeleteRetentionPolicy	Concede permissão para excluir a política de retenção com base na organização fornecida e nos identificadores da política.	Write	organization*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteSmtpGateway [somente permissão]	Concede permissão para remover um gateway SMTP de uma organização.	Gravar	organization*		
DeleteUser	Concede permissão para excluir um usuário de todos WorkMail os sistemas subsequentes	Gravar	organization*		
DeliverToMailbox [somente permissão]	Concede permissão para entregar e-mails a uma WorkMail organização por meio da MailManager DeliverToMailbox ação SES	Gravar	organization*		
DeregisterFromWorkMail	Concede permissão para marcar um usuário, grupo ou recurso como não mais usado no WorkMail	Gravar	organization*		
DeregisterMailDomain	Concede permissão para remover o registro de um domínio de e-mail de uma organização	Gravar	organization*		
DescribeEmailMonitoringConfiguration	Concede permissão para recuperar a configuração de monitoramento de e-mail de uma organização	Leitura	organization*		
DescribeEntity	Concede permissão para ler detalhes de uma entidade	Leitura	organization*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeGroup	Concede permissão para ler os detalhes de um grupo.	Lista	organization*		
DescribeIdentityProviderConfiguration	Concede permissão para ler a configuração do provedor de identidade para a organização	Leitura	organization*		
DescribeInboundDmarcSettings	Concede permissão para ler as configurações em uma política de DMARC para uma organização especificada	Leitura	organization*		
DescribeInboundMailFlowRule [somente permissão]	Concede permissão para ler os detalhes de uma regra de fluxo de e-mails de entrada configurada para uma organização.	Read	organization*		
DescribeMailDomains [somente permissão]	Concede permissão para mostrar os detalhes de todos os domínios de e-mail associados à organização.	Lista	organization*		
DescribeMailboxExportJob	Concede permissão para recuperar detalhes de um trabalho de exportação de caixa postal.	Read	organization*		
DescribeOrganization	Concede permissão para ler os detalhes de uma organização.	List	organization*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeOutboundMailFlowRule [somente permissão]	Concede permissão para ler os detalhes de uma regra de fluxo de e-mails de saída configurada para uma organização.	Read	organization*		
DescribeResource	Concede permissão para ler os detalhes de um recurso	List	organization*		
DescribeSmtpGateway [somente permissão]	Concede permissão para ler os detalhes de um gateway SMTP registrado em uma organização.	Read	organization*		
DescribeUser	Concede permissão para ler detalhes de um usuário.	Lista	organization*		
DisassociateDelegateFromResource	Concede permissão para remover um membro do conjunto de delegados do recurso.	Write	organization*		
DisassociateMemberFromGroup	Concede permissão para remover um membro de um grupo.	Write	organization*		
EnableMailDomain [somente permissão]	Concede permissão para habilitar um domínio de e-mail na organização.	Gravar	organization*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAccessControlEffect	Concede permissão para obter os efeitos das regras de controle de acesso conforme elas se aplicam a um IPv4 endereço específico, ação de protocolo de acesso ou ID de usuário	Leitura	organization*		
GetDefaultRetentionPolicy	Concede permissão para recuperar a política de retenção associada a um nível organizacional.	Leitura	organization*		
GetImpersonationRole	Concede permissão para recuperar uma função de falsificação de identidade para uma determinada organização da Amazon WorkMail	Leitura	organization*		
GetImpersonationRoleEffect	Concede permissão para obter o efeito das regras associadas a uma função de representação para um usuário específico	Leitura	organization*		
GetJournalingRules [somente permissão]	Concede permissão para ler os endereços de e-mail configurados de registro e fallback para o registro de e-mail.	Leitura	organization*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetMailDomain	Concede permissão para recuperar detalhes de um determinado domínio de e-mail em uma organização	Leitura	organization*		
GetMailDomainDetails [somente permissão]	Concede permissão para obter os detalhes do domínio de e-mail.	Leitura	organization*		
GetMailboxDetails	Concede permissão para ler os detalhes da caixa postal do usuário.	Read	organization*		
GetMobileDeviceAccessEffect	Concede permissão para simular o efeito das regras de acesso por dispositivos móveis para os atributos determinados de um evento de acesso de exemplo.	Leitura	organization*		
GetMobileDeviceAccessOverride	Concede permissão para recuperar uma sobreposição de um acesso de dispositivo móvel	Leitura	organization*		
GetMobileDeviceDetails [somente permissão]	Concede permissão para obter os detalhes do dispositivo móvel.	Read	organization*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetMobileDevicesForUser [somente permissão]	Concede permissão para obter uma lista dos dispositivos móveis associados ao usuário.	Read	organization*		
GetMobilePolicyDetails [somente permissão]	Concede permissão para obter os detalhes da política de dispositivos móveis associada à organização.	Leitura	organization*		
GetPersonalAccessTokenMetadata	Concede permissão para ler metadados de um token de acesso pessoal	Leitura	organization*		
ListAccessControlRules	Concede permissão para listar as regras de controle de acesso.	Leitura	organization*		
ListAliases	Concede permissão para listar os aliases associados a determinada entidade.	Lista	organization*		
ListAvailabilityConfigurations	Concede permissão para listar todos os AvailabilityConfiguration itens de uma determinada WorkMail organização da Amazon	Leitura	organization*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListGroupMembers	Concede permissão para ler uma visão geral dos membros de um grupo. Usuários e grupos podem ser membros de um grupo.	List	organization*		
ListGroups	Concede permissão para listar os resumos dos grupos da organização.	Lista	organization*		
ListGroupsForEntity	Concede permissão para listar os grupos aos quais uma entidade pertence	Lista	organization*		
ListImpersonationRoles	Concede permissão para listar as funções de falsificação de identidade de uma determinada organização da Amazon WorkMail	Lista	organization*		
ListInboundMailFlowRules [somente permissão]	Concede permissão para listar as regras de fluxo de e-mails de entrada configuradas para uma organização.	Lista	organization*		
ListMailDomains	Concede permissão para listar o domínio de e-mail de uma determinada organização	Lista	organization*		
ListMailboxExportJobs	Concede permissão para listar os trabalhos de exportação de caixa postal.	List	organization*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListMailboxPermissions	Concede permissão para listar as permissões da caixa postal associadas a um usuário, a um grupo ou a uma caixa postal de recurso.	Lista	organization*		
ListMobileDeviceAccessOverrides	Concede permissão para listar as sobreposições de acesso por dispositivos móveis	Leitura	organization*		
ListMobileDeviceAccessRules	Concede permissão para listar as regras de acesso por dispositivos móveis.	Leitura	organization*		
ListOrganizations	Concede permissão para listar as organizações não excluídas.	List			
ListOutboundMailFlowRules [somente permissão]	Concede permissão para listar as regras de fluxo de e-mails recebidos configuradas para uma organização.	Lista	organization*		
ListPersonalAccessTokens	Concede permissão para listar metadados para tokens de acesso pessoal	Lista	organization*		
ListResourceDelegates	Concede permissão para listar os delegados associados a um recurso.	List	organization*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListResources	Concede permissão para listar os recursos da organização	List	organization*		
ListSmtpGateways [somente permissão]	Concede permissão para listar gateways SMTP registrados na organização.	Lista	organization*		
ListTagsForResource	Concede permissão para listar as tags aplicadas a um recurso WorkMail organizacional da Amazon	Lista	organization*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ListUsers	Concede permissão para listar os usuários da organização	List	organization*		
PutAccessControlRule	Concede permissão para adicionar uma nova regra de controle de acesso.	Gravar	organization*		
PutEmailMonitoringConfiguration	Concede permissão para adicionar ou atualizar a configuração de monitoramento de e-mail de uma organização	Gravar	organization*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutIdentityProviderConfiguration	Concede permissão para adicionar ou atualizar a configuração do provedor de identidade para a organização	Gravar	organization*		
PutInboundDmarcSettings	Concede permissão para habilitar ou desabilitar uma política de DMARC para uma determinada organização	Gravar	organization*		
PutMailboxPermissions	Concede permissão para definir as permissões de um usuário, grupo ou recurso, substituindo as permissões existentes.	Gravar	organization*		
PutMobileDeviceAccessOverride	Concede permissão para adicionar ou atualizar uma sobreposição de acesso de dispositivo móvel	Gravar	organization*		
PutRetentionPolicy	Concede permissão para adicionar ou atualizar a política de retenção.	Gravar	organization*		
RegisterMailDomain	Concede permissão para registrar um novo domínio de e-mail de uma organização	Gravar	organization*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
RegisterToWorkMail	Concede permissão para registrar um usuário, um grupo ou um recurso existente e desabilitado para uso associando uma caixa postal e recursos de calendário.	Gravar	organization*		
ResetPassword	Concede permissão para permitir que o administrador redefina a senha de um usuário.	Write	organization*		
SearchMembers [somente permissão]	Concede permissão para realizar uma pesquisa de prefixo para localizar um usuário específico em um grupo de e-mails.	Read	organization*		
SetDefaultMailDomain [somente permissão]	Concede permissão para definir o domínio-padrão de e-mail da organização.	Write	organization*		
SetJournalingRules [somente permissão]	Concede permissão para definir os endereços de e-mail de registro e fallback do registro de e-mail.	Write	organization*		
SetMobilePolicyDetails [somente permissão]	Concede permissão para definir os detalhes de uma política de dispositivos móveis associada à organização.	Write	organization*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartMailboxExportJob	Concede permissão para iniciar um novo trabalho de exportação de caixa postal.	Gravar	organization*		
TagResource	Concede permissão para marcar o recurso específico WorkMail da organização Amazon	Tags	organization*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TestAvailabilityConfiguration	Concede permissão para realizar um teste em um provedor de disponibilidade para garantir que o acesso seja permitido	Leitura	organization*		
TestInboundMailFlowRules [somente permissão]	Concede permissão para testar quais regras de entrada serão aplicadas a um e-mail com determinado remetente e destinatário.	Write	organization*		
TestOutboundMailFlowRules [somente permissão]	Concede permissão para testar quais regras de saída serão aplicadas a um e-mail com determinado remetente e destinatário.	Gravar	organization*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UntagResource	Concede permissão para desmarcar o recurso específico da WorkMail organização Amazon	Tags	organization*		
				aws:TagKeys	
UpdateAvailabilityConfiguration	Concede permissão para atualizar uma WorkMail organização e domínio existentes AvailabilityConfiguration para a Amazon em questão	Gravar	organization*		
UpdateDefaultMailDomain	Concede permissão para atualizar qual domínio é o domínio padrão para uma organização	Gravar	organization*		
UpdateGroup	Concede permissão para atualizar os detalhes de um grupo	Gravar	organization*		
UpdateImpersonationRole	Concede permissão para atualizar uma função de representação existente para uma determinada organização da Amazon WorkMail	Gravar	organization*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateInboundMailFlowRule [somente permissão]	Concede permissão para atualizar os detalhes de uma regra de fluxo de e-mails de entrada que será aplicada a todos os e-mails enviados para uma organização.	Write	organization*		
UpdateMailboxQuota	Concede permissão para atualizar o tamanho máximo (em MB) da caixa postal do usuário.	Gravar	organization*		
UpdateMobileDeviceAccessRule	Concede permissão para atualizar uma regra de acesso por dispositivos móveis	Gravar	organization*		
UpdateOutboundMailFlowRule [somente permissão]	Concede permissão para atualizar os detalhes de uma regra de fluxo de e-mails recebidos que será aplicada a todos os e-mails enviados de uma organização.	Write	organization*		
UpdatePrimaryEmailAddress	Concede permissão para atualizar o e-mail principal de um usuário, grupo ou recurso.	Write	organization*		
UpdateResource	Concede permissão para atualizar os detalhes do recurso.	Write	organization*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateSmtpGateway [somente permissão]	Concede permissão para atualizar os detalhes de um gateway SMTP existente registrado em uma organização.	Gravar	organization*		
UpdateUser	Concede permissão para atualizar os detalhes de um usuário	Gravar	organization*		
WipeMobileDevice [somente permissão]	Concede permissão para limpar remotamente o dispositivo móvel associado à conta de um usuário.	Gravar	organization*		

Tipos de recursos definidos pela Amazon WorkMail

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
organization	`arn:${Partition}:workmail:${Region}:${Account}:organization/${ResourceId}`	aws:ResourceTag/${TagKey}

Chaves de condição para Amazon WorkMail

A Amazon WorkMail define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelos pares de chave-valor da etiqueta que são transmitidos na solicitação	String
aws:ResourceTag/${TagKey}	Filtra o acesso por pares chave-valor da etiqueta anexados ao recurso	String
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o Amazon WorkMail Message Flow

O Amazon WorkMail Message Flow (prefixo do serviço:`workmailmessageflow`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon WorkMail Message Flow
- Tipos de recursos definidos pelo Amazon WorkMail Message Flow
- Chaves de condição para o Amazon WorkMail Message Flow

Ações definidas pelo Amazon WorkMail Message Flow

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de

recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetRawMessageContent	Concede permissão para ler o conteúdo de mensagens de e-mail com o ID de mensagem especificado	Leitura	RawMessage*		
PutRawMessageContent	Concede permissão para atualizar o conteúdo das mensagens de e-mail com o ID da mensagem especificado	Gravar	RawMessage*		

Tipos de recursos definidos pelo Amazon WorkMail Message Flow

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
RawMessage	`arn:${Partition}:workmailmessageflow:${Region}:${Account}:message/${OrganizationId}/${Context}/${MessageId}`	

Chaves de condição para o Amazon WorkMail Message Flow

WorkMail O fluxo de mensagens não tem chaves de contexto específicas do serviço que possam ser usadas no `Condition` elemento das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para a Amazon WorkSpaces

A Amazon WorkSpaces (prefixo do serviço:`workspaces`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pela Amazon WorkSpaces
- Tipos de recursos definidos pela Amazon WorkSpaces
- Chaves de condição para Amazon WorkSpaces

Ações definidas pela Amazon WorkSpaces

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando

usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AcceptAccountLinkInvitation	Concede permissão para aceitar convites de outras AWS contas para compartilhar a mesma configuração para BYOL WorkSpaces	Gravar			
AssociateConnectionAlias	Concede permissão para associar aliases de conexão a diretórios.	Write	connectionalias*		
			directoryid*		
AssociateIpGroups	Concede permissão para associar grupos de controle de acesso IP a diretórios.	Gravar	directoryid*		
			workspaceipgroup*		
AssociateWorkspaceApplication	Concede permissão para associar um aplicativo de espaço de trabalho a um WorkSpace	Gravar	workspaceapplication*		
			workspaceid*		
				aws:ResourceTag/${TagKey}	
AuthorizeIpRules	Concede permissão para adicionar regras a grupos de controle de acesso IP.	Gravar	workspaceipgroup*		workspaces:UpdateRulesOfIpGroup

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CopyWorkspaceImage	Concede permissão para copiar uma WorkSpace imagem	Gravar	workspaceimage*		workspaces:DescribeWorkspaceImages
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAccountLinkInvitation	Concede permissão para convidar outras AWS contas para compartilhar a mesma configuração para WorkSpaces BYOL	Gravar			
CreateConnectClientAddIn	Concede permissão para criar um suplemento do cliente do Amazon Connect em um diretório	Gravar	directoryid*		
CreateConnectionAlias	Concede permissão para criar aliases de conexão para uso com redirecionamento entre regiões.	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateIpGroup	Concede permissão para criar grupos de controle de acesso IP.	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRootClientCertificate [somente permissão]	Concede permissão para criar um certificado de cliente raiz	Gravar	certificateid*		
CreateStandbyWorkspaces	Concede permissão para criar um ou mais Standby WorkSpaces	Gravar	directoryid*		
			workspaceid*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTags	Concede permissão para criar tags para WorkSpaces recursos	Tags		aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateUpdatedWorkspaceImage	Concede permissão para criar uma WorkSpace imagem atualizada	Gravar	workspace image*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspaceBundle	Concede permissão para criar um WorkSpace pacote	Gravar	workspace bundle*		workspaces:CreateTags
			workspace image*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspaceImage	Concede permissão para criar uma nova WorkSpace imagem	Gravar	workspace id*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateWorkspaces	Concede permissão para criar um ou mais WorkSpaces	Gravar	directoryid*		
			workspacebundle*		
			workspaceid*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspacesPool	Concede permissão para criar um WorkSpaces Pool	Gravar	directoryid*		
			workspacebundle*		
			workspacespoolid*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteAccountLinkInvitation	Concede permissão para excluir convites para que outras AWS contas compartilhem a mesma configuração para BYOL WorkSpaces	Gravar			
DeleteClientBranding	Concede permissão para excluir dados de identidade visual do AWS WorkSpaces cliente em um diretório	Gravar	directoryid*		
DeleteConnectClientAddIn	Concede permissão para excluir um suplemento do cliente do Amazon Connect configurado em um diretório	Gravar	directoryid*		
DeleteConnectionAlias	Concede permissão para excluir aliases de conexão.	Write	connectionalias*		
DeleteIpGroup	Concede permissão para excluir grupos de controle de acesso IP.	Gravar	workspaceipgroup*		
DeleteRootClientCertificate [somente permissão]	Concede permissão para excluir o certificado do cliente raiz	Gravar	certificateid*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteTags	Concede permissão para excluir tags dos WorkSpaces recursos	Tags		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteWorkspaceBundle	Concede permissão para excluir WorkSpace pacotes	Gravar	workspacebundle*		
DeleteWorkspaceImage	Concede permissão para excluir WorkSpace imagens	Gravar	workspaceimage*		
DeployWorkspaceApplications	Concede permissão para implantar todos os aplicativos de espaço de trabalho pendentes em um WorkSpace	Gravar	workspaceid*		
				aws:ResourceTag/${TagKey}	
DeregisterWorkspaceDirectory	Concede permissão para cancelar o registro de diretórios e não serem usados na Amazon WorkSpaces	Gravar	directoryid*		
DescribeAccount	Concede permissão para recuperar a configuração do Bring Your Own License (BYOL) para contas WorkSpaces	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeAccountModifications	Concede permissão para recuperar modificações na configuração do Bring Your Own License (BYOL) para contas WorkSpaces	Leitura			
DescribeApplicationAssociations	Concede permissão para recuperar informações sobre recursos associados a um aplicativo WorkSpace	Lista	workspaceapplication*		
				aws:ResourceTag/${TagKey}	
DescribeApplications	Concede permissão para obter informações sobre WorkSpace aplicativos	Lista			
DescribeBundleAssociations	Concede permissão para recuperar informações sobre recursos associados a um pacote WorkSpace	Lista	workspacebundle*		
				aws:ResourceTag/${TagKey}	
DescribeClientBranding	Concede permissão para recuperar dados da marca AWS WorkSpaces do cliente em um diretório	Leitura	directoryid*		
DescribeClientProperties	Concede permissão para recuperar informações sobre clientes WorkSpaces	Lista	directoryid*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeConnectClientAddIns	Concede permissão para recuperar uma lista de suplementos de cliente do Amazon Connect que foram criados	Lista	directoryid*		
DescribeConnectionAliasPermissions	Concede permissão para recuperar as permissões que os proprietários dos aliases de conexão concederam a outras AWS contas para aliases de conexão	Leitura	connectionalias*		
DescribeConnectionAliases	Concede permissão para recuperar uma lista que descreve os aliases de conexão usados para o redirecionamento entre regiões.	Leitura			
DescribeConsent [somente permissão]	Concede permissão para recuperar informações sobre o contrato de consentimento com os requisitos mínimos do BYOL	Leitura			
DescribeCustomWorkspaceImageImport	Concede permissão para recuperar informações sobre a tarefa de importação de imagem WorkSpace BYOL	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeImageAssociations	Concede permissão para recuperar informações sobre recursos associados a uma imagem WorkSpace	Lista	workspaceimage*		
				aws:ResourceTag/${TagKey}	
DescribeIpGroups	Concede permissão para recuperar informações sobre grupos de concede de acesso IP.	Leitura	workspaceipgroup*		
DescribeRootClientCertificates [somente permissão]	Concede permissão para recuperar informações para certificados de cliente raiz	Lista	certificateid*		
DescribeTags	Concede permissão para descrever as tags WorkSpaces dos recursos	Leitura			
DescribeWorkspaceAssociations	Concede permissão para recuperar informações sobre recursos associados a um WorkSpace	Lista	workspaceid*		
				aws:ResourceTag/${TagKey}	
DescribeWorkspaceBundles	Concede permissão para obter informações sobre WorkSpace pacotes	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeWorkspaceDirectories	Concede permissão para recuperar informações sobre diretórios registrados com WorkSpaces	Leitura			
DescribeWorkspaceImagePermissions	Concede permissão para recuperar informações sobre permissões de WorkSpace imagem	Leitura	workspace image*		
DescribeWorkspaceImages	Concede permissão para recuperar informações sobre imagens WorkSpace	Lista			
DescribeWorkspaceSnapshots	Concede permissão para recuperar informações sobre instantâneos WorkSpace	Lista	workspace id*		
DescribeWorkspaces	Concede permissão para obter informações sobre WorkSpaces	Lista			
DescribeWorkspacesConnectionStatus	Concede permissão para obter o status da conexão de WorkSpaces	Leitura			
DescribeWorkspacesPoolSessions	Concede permissão para recuperar informações sobre as sessões de um pool WorkSpaces	Lista	workspace spoolid*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DescribeWorkspacesPools	Concede permissão para recuperar informações sobre pools WorkSpaces	Lista			
DirectoryAccessManagement [somente permissão]	Concede permissão para ações de gerenciamento de diretórios ao gerenciar e provisionar espaços de trabalho	Lista	directoryid*		
DisassociateConnectionAlias	Concede permissão para desassociar aliases de conexão de diretórios.	Write	connectionalias*		
DisassociateIpGroups	Concede permissão para desassociar grupos de controle de acesso IP dos diretórios.	Gravar	directoryid*		
			workspaceipgroup*		
DisassociateWorkspaceApplication	Concede permissão para desassociar um aplicativo de espaço de trabalho de um WorkSpace	Gravar	workspaceapplication*		
			workspaceid*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetAccountLink	Concede permissão para recuperar um link com outra AWS conta para compartilhar a configuração para BYOL WorkSpaces	Leitura			
ImportClientBranding	Concede permissão para importar dados de identidade visual do AWS WorkSpaces cliente em um diretório	Gravar	directoryid*		
ImportCustomWorkspaceImage	Concede permissão para importar imagens Bring Your Own License (BYOL) para a Amazon WorkSpaces	Gravar			
ImportWorkspaceImage	Concede permissão para importar imagens Bring Your Own License (BYOL) para a Amazon WorkSpaces	Gravar			ec2:DescribeImages ec2:ModifyImageAttribute
ListAccountLinks	Concede permissão para recuperar links com a (s) AWS conta (s) que compartilham sua configuração para BYOL WorkSpaces	Lista			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListAvailableManagementCidrRanges	Concede permissão para listar os intervalos de CIDR disponíveis para ativar o Bring Your Own License (BYOL) para contas WorkSpaces	Lista			
MigrateWorkspace	Concede permissão para migrar WorkSpaces	Gravar	workspacebundle*		
			workspaceid*		
ModifyAccount	Concede permissão para modificar a configuração do Bring Your Own License (BYOL) para contas WorkSpaces	Gravar			
ModifyCertificateBasedAuthProperties	Concede permissão para modificar as propriedades de autorização baseadas em certificado de um diretório	Gravar	directoryid*		
ModifyClientProperties	Concede permissão para modificar as propriedades dos WorkSpaces clientes	Gravar	directoryid*		
ModifyEndpointEncryptionMode	Concede permissão para configurar o diretório especificado entre o modo validado por TLS padrão e FIPS 140-2	Gravar	directoryid*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ModifySamlProperties	Concede permissão para modificar as propriedades de SAML de um diretório	Gravar	directory id*		
ModifySelfservicePermissions	Concede permissão para modificar os recursos de WorkSpace gerenciamento de autoatendimento para seus usuários	Gerenciamento de permissões	directory id*		
ModifyStreamingProperties	Concede permissão para modificar as propriedades de streaming	Gravar	directory id*		
ModifyWorkspaceAccessProperties	Concede permissão para especificar quais dispositivos e sistemas operacionais os usuários podem usar para acessar seus WorkSpaces	Gravar	directory id*		
ModifyWorkspaceCreationProperties	Concede permissão para modificar as propriedades padrão usadas para criar WorkSpaces	Gravar	directory id*		
ModifyWorkspaceProperties	Concede permissão para modificar WorkSpace propriedades, incluindo o modo de execução e o AutoStop período	Gravar	workspace id*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ModifyWorkspaceState	Concede permissão para modificar o estado de WorkSpaces	Gravar	workspaceid*		
RebootWorkspaces	Concede permissão para reinicializar WorkSpaces	Gravar	workspaceid*		
RebuildWorkspaces	Concede permissão para reconstruir WorkSpaces	Gravar	workspaceid*		
RegisterWorkspaceDirectory	Concede permissão para registrar diretórios para uso com a Amazon WorkSpaces	Gravar	directoryid*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RejectAccountLinkInvitation	Concede permissão para rejeitar convites de outras AWS contas para compartilhar a mesma configuração para BYOL WorkSpaces	Gravar			
RestoreWorkspace	Concede permissão para restaurar WorkSpaces	Gravar	workspaceid*		
RevokeIpRules	Concede permissão para remover regras de grupos de controle de acesso IP.	Gravar	workspaceipgroup*		workspaces:UpdateRulesOfIpGroup

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
StartWorkspaces	Concede permissão para começar AutoStop WorkSpaces	Gravar	workspaceid*		
StartWorkspacesPool	Concede permissão para iniciar um WorkSpaces pool	Gravar	workspacespoolid*		
StopWorkspaces	Concede permissão para parar AutoStop WorkSpaces	Gravar	workspaceid*		
StopWorkspacesPool	Concede permissão para parar uma WorkSpaces piscina	Gravar	workspacespoolid*		
Stream	Concede permissão para usuários federados fazerem login usando as credenciais existentes e transmitirem seu workspace	Gravar	directoryid*		
				workspaces:userId	
TerminateWorkspaces	Concede permissão para rescindir WorkSpaces	Gravar	workspaceid*		
TerminateWorkspacesPool	Concede permissão para encerrar um pool WorkSpaces	Gravar	workspacespoolid*		
TerminateWorkspacesPoolSession	Concede permissão para encerrar uma sessão de WorkSpaces Pool	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateConnectClientAddIn	Concede permissão para atualizar um suplemento do cliente do Amazon Connect. Use esta ação para atualizar o nome e o URL do endpoint de um suplemento do cliente do Amazon Connect	Gravar	directoryid*		
UpdateConnectionAliasPermission	Concede permissão para compartilhar ou cancelar o compartilhamento de aliases de conexão com outras contas.	Gerenciamento de permissões	connectionalias*		
UpdateConsent [somente permissão]	Concede permissão para atualizar o contrato de consentimento de acordo com os requisitos mínimos do BYOL	Gravar			
UpdateRootClientCertificate [somente permissão]	Concede permissão para atualizar um certificado de cliente raiz	Gravar	certificateid*		
UpdateRulesOfIpGroup	Concede permissão para substituir regras de grupos de controle de acesso IP.	Gravar	workspaceipgroup*		workspaces:AuthorizeIpRules workspaces:RevokeIpRules

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateWorkspaceBundle	Concede permissão para atualizar as WorkSpace imagens usadas nos WorkSpace pacotes	Gravar	workspacebundle*		
			workspaceimage*		
UpdateWorkspaceImagePermission	Concede permissão para compartilhar ou cancelar o compartilhamento de WorkSpace imagens com outras contas especificando se outras contas têm permissão para copiar a imagem	Gerenciamento de permissões	workspaceimage*		
UpdateWorkspacesPool	Concede permissão para atualizar o WorkSpaces pool	Gravar	workspacespoolid*		

Tipos de recursos definidos pela Amazon WorkSpaces

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
certificateid	arn:${Partition}:workspaces:${Region}:${Account}:workspacecertificate/${CertificateId}	
directoryid	arn:${Partition}:workspaces:${Region}:${Account}:directory/${DirectoryId}	aws:ResourceTag/${TagKey}
workspacebundle	arn:${Partition}:workspaces:${Region}:${Account}:workspacebundle/${BundleId}	aws:ResourceTag/${TagKey}
workspaceid	arn:${Partition}:workspaces:${Region}:${Account}:workspace/${WorkspaceId}	aws:ResourceTag/${TagKey}
workspaceimage	arn:${Partition}:workspaces:${Region}:${Account}:workspaceimage/${ImageId}	aws:ResourceTag/${TagKey}
workspaceipgroup	arn:${Partition}:workspaces:${Region}:${Account}:workspaceipgroup/${GroupId}	aws:ResourceTag/${TagKey}
workspacespoolid	arn:${Partition}:workspaces:${Region}:${Account}:workspacespool/${PoolId}	aws:ResourceTag/${TagKey}
connectionalias	arn:${Partition}:workspaces:${Region}:${Account}:connectionalias/${ConnectionAliasId}	aws:ResourceTag/${TagKey}
workspaceapplication	arn:${Partition}:workspaces:${Region}:${Account}:workspaceapplication/${WorkSpaceApplicationId}	aws:ResourceTag/${TagKey}

Chaves de condição para Amazon WorkSpaces

A Amazon WorkSpaces define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base nas etiquetas transmitidas na solicitação	String
aws:ResourceTag/${TagKey}	Filtra as ações com base nas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra ações com base nas chaves da etiqueta transmitidas na solicitação	ArrayOfString
workspaces:userId	Filtra o acesso pelo ID do usuário de Workspaces	String

Ações, recursos e chaves de condição para o Amazon WorkSpaces Application Manager

O Amazon WorkSpaces Application Manager (prefixo do serviço:`wam`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.

- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon WorkSpaces Application Manager
- Tipos de recursos definidos pelo Amazon WorkSpaces Application Manager
- Chaves de condição para o Amazon WorkSpaces Application Manager

Ações definidas pelo Amazon WorkSpaces Application Manager

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AuthenticatePackager [somente permissão]	Permite que a instância de empacotamento do Amazon WAM acesse o catálogo de pacotes de aplicativos.	Gravar			

Tipos de recursos definidos pelo Amazon WorkSpaces Application Manager

O Amazon WorkSpaces Application Manager não suporta a especificação de um ARN de recurso no elemento de uma `Resource` declaração de política do IAM. Para permitir o acesso ao Amazon WorkSpaces Application Manager, especifique `"Resource": "*"` em sua política.

Chaves de condição para o Amazon WorkSpaces Application Manager

O WAM não tem chaves de contexto específicas ao serviço que podem ser usadas no elemento `Condition` das declarações de política. Para ver a lista das chaves de contexto globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Ações, recursos e chaves de condição para instâncias AWS WorkSpaces gerenciadas

AWS WorkSpaces As instâncias gerenciadas (prefixo do serviço:`workspaces-instances`) fornecem os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas por instâncias AWS WorkSpaces gerenciadas
- Tipos de recursos definidos por instâncias AWS WorkSpaces gerenciadas
- Chaves de condição para instâncias AWS WorkSpaces gerenciadas

Ações definidas por instâncias AWS WorkSpaces gerenciadas

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar

a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateVolume	Concede permissão para associar um volume gerenciado do espaço de trabalho a uma instância gerenciada do espaço de trabalho na sua conta	Gravar	WorkspaceInstanceId*		ec2:AttachVolume ec2:DescribeVolumes
CreateVolume	Concede permissão para criar um volume gerenciado pelo espaço de trabalho em sua conta	Gravar			ec2:CreateVolume

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateWorkspaceInstance	Concede permissão para criar uma instância gerenciada por espaço de trabalho em sua conta	Gravar		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeInstances ec2:RunInstances
DeleteVolume	Concede permissão para excluir um volume gerenciado pelo espaço de trabalho em sua conta	Gravar	VolumeId*		ec2:DeleteVolume ec2:DescribeVolumes
DeleteWorkspaceInstance	Concede permissão para excluir uma instância gerenciada do espaço de trabalho em sua conta	Gravar	WorkspaceInstanceId*		ec2:TerminateInstances
DisassociateVolume	Concede permissão para desassociar um volume gerenciado por espaço de trabalho de uma instância gerenciada por espaço de trabalho em sua conta	Gravar	WorkspaceInstanceId*		ec2:DescribeVolumes ec2:DetachVolume
GetWorkspaceInstance	Concede permissão para obter detalhes de uma instância gerenciada de espaço de trabalho específica em sua conta	Leitura	WorkspaceInstanceId*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListInstanceTypes	Concede permissão para listar todos os tipos de instância compatíveis	Lista			
ListRegions	Concede permissão para listar todas as AWS regiões suportadas	Lista			
ListTagsForResource	Concede permissão para listar tags de usuário para recursos em sua conta	Lista	WorkspaceInstanceId*		
ListWorkspaceInstances	Concede permissão para listar instâncias gerenciadas pelo espaço de trabalho em sua conta	Lista			
TagResource	Concede permissão para adicionar tags de usuário aos recursos da sua conta	Tags	WorkspaceInstanceId*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Concede permissão para remover tags de usuário dos recursos da sua conta	Tags	WorkspaceInstanceId*		
				aws:TagKeys	

Tipos de recursos definidos por instâncias AWS WorkSpaces gerenciadas

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
WorkspaceInstanceId	`arn:${Partition}:workspaces-instances:${Region}:${Account}:workspaceinstance/${WorkspaceInstanceId}`	aws:ResourceTag/${TagKey}
VolumeId	`arn:${Partition}:ec2:${Region}:${Account}:volume/${VolumeId}`	aws:ResourceTag/${TagKey}

Chaves de condição para instâncias AWS WorkSpaces gerenciadas

AWS WorkSpaces As instâncias gerenciadas definem as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Type
aws:RequestTag/${TagKey}	Filtra ações com base nas etiquetas transmitidas na solicitação	String

Chaves de condição	Descrição	Type
aws:ResourceTag/${TagKey}	Filtra as ações com base nas etiquetas associadas ao recurso	String
aws:TagKeys	Filtra ações com base nas chaves da etiqueta transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o Amazon WorkSpaces Secure Browser

O Amazon WorkSpaces Secure Browser (prefixo do serviço:`workspaces-web`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon WorkSpaces Secure Browser
- Tipos de recursos definidos pelo Amazon WorkSpaces Secure Browser
- Chaves de condição para o Amazon WorkSpaces Secure Browser

Ações definidas pelo Amazon WorkSpaces Secure Browser

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla

o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
AssociateBrowserSettings	Concede permissão para associar configurações do navegador a portais da web	Gravar	browserSettings*		
			portal*		
AssociateDataProtectionSettings	Concede permissão para associar configurações de proteção de dados a portais da web	Gravar	dataProtectionSettings*		
			portal*		
AssociateIpAccessSettings	Concede permissão para associar configurações de acesso IP a portais da web	Gravar	ipAccessSettings*		
			portal*		
AssociateNetworkSettings	Concede permissão para associar configurações de rede a portais da Web	Gravar	networkSettings*		ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateTags ec2:DeleteNetworkInterface ec2:DeleteNetworkI

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
					nterfaceP ermission ec2:Modif yNetworkI nterfaceA ttribute
			portal*		
Associate SessionLo gger	Concede permissão para associar o registrador de sessão a portais da web	Gravar	portal*		
			sessionLo gger*		
Associate TrustStore	Concede permissão para associar lojas de confiança a portais da web	Gravar	portal*		
			trustStor e*		
Associate UserAcces sLoggingS ettings	Concede permissão para associar configurações do usuário a portais da web	Gravar	portal*		kinesis:P utRecord kinesis:P utRecords
			userAcces sLoggingS ettings*		
Associate UserSettings	Concede permissão para associar configurações do usuário a portais da web	Gravar	portal*		
			userSetti ngs*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateBrowserSettings	Concede permissão para criar configurações de navegador	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey
CreateDataProtectionSettings	Concede permissão para criar configurações de proteção de dados	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
CreateIdentityProvider	Concede permissão para criar provedores de identidade	Gravar	identityProvider* portal*	aws:TagKeys aws:RequestTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateIpAccessSettings	Concede permissão para criar as configurações de acesso IP	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
CreateNetworkSettings	Concede permissão para criar configurações de rede	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
CreatePortal	Concede permissão para criar portais da Web	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateSessionLogger	Concede permissão para criar um registrador de sessão	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
CreateTrustStore	Concede permissão para criar armazenamento de trust	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
CreateUserAccessLoggingSettings	Concede permissão para criar configurações de registro de acesso de usuário	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
CreateUserSettings	Concede permissão para criar configurações de usuário	Gravar		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteBrowserSettings	Concede permissão para excluir configurações do navegador	Gravar	browserSettings*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteDataProtectionSettings	Concede permissão para excluir configurações de proteção de dados	Gravar	dataProtectionSettings*		
DeleteIdentityProvider	Concede permissão para excluir provedores de identidade	Gravar	identityProvider*		
			portal*		
DeleteIpAccessSettings	Concede permissão para excluir as configurações de acesso IP	Gravar	ipAccessSettings*		
DeleteNetworkSettings	Concede permissão para excluir configurações de rede	Gravar	networkSettings*		
DeletePortal	Concede permissão para excluir portais da web	Gravar	portal*		
DeleteSessionLogger	Concede permissão para excluir o registrador de sessão	Gravar	sessionLogger*		
DeleteTrustStore	Concede permissão para excluir armazenamento de trust	Gravar	trustStore*		
DeleteUserAccessLoggingSettings	Concede permissão para excluir configurações de registro de acesso	Gravar	userAccessLoggingSettings*		
DeleteUserSettings	Concede permissão para excluir configurações de usuário	Gravar	userSettings*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateBrowserSettings	Concede permissão para desassociar as configurações do navegador de portais da web	Gravar	portal*		
DisassociateDataProtectionSettings	Concede permissão para desassociar o registro de proteção de dados dos portais da web	Gravar	portal*		
DisassociateIpAccessSettings	Concede permissão para desassociar o registro de acesso IP de portais da web	Gravar	portal*		
DisassociateNetworkSettings	Concede permissão para desassociar configurações de rede de portais da web	Gravar	portal*		
DisassociateSessionLogger	Concede permissão para desassociar o registrador de sessão dos portais da web	Gravar	portal*		
DisassociateTrustStore	Concede permissão para desassociar armazenamento de trust de portais da web	Gravar	portal*		
DisassociateUserAccessLoggingSettings	Concede permissão para desassociar as configurações de usuário de portais da web	Gravar	portal*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DisassociateUserSettings	Concede permissão para desassociar as configurações de usuário de portais da web	Gravar	portal*		
ExpireSession	Concede permissão para expirar uma sessão de um portal específico	Gravar	portal*		
GetBrowserSettings	Concede permissão para obter detalhes sobre as configurações do navegador	Leitura	browserSettings*		
GetDataProtectionSettings	Concede permissão para obter detalhes sobre as configurações de proteção de dados	Leitura	dataProtectionSettings*		
GetIdentityProvider	Concede permissão para obter detalhes sobre provedores de identidade	Leitura	identityProvider*		
GetIpAccessSettings	Concede permissão para obter detalhes sobre as configurações de acesso IP	Leitura	ipAccessSettings*		
GetNetworkSettings	Concede permissão para obter detalhes sobre as configurações de rede	Leitura	networkSettings*		
GetPortal	Concede permissão para obter detalhes sobre portais da web	Leitura	portal*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetPortalServiceProviderMetadata	Concede permissão para obter informações de metadados do provedor de serviços para portais da web	Leitura	portal*		
GetSession	Concede permissão para obter informações sobre uma sessão em particular de um portal	Leitura	portal*		
GetSessionLogger	Concede permissão para obter detalhes sobre o registrador de sessão	Leitura	sessionLogger*		
GetTrustStore	Concede permissão para obter detalhes sobre armazenamentos de trust	Leitura	trustStore*		
GetTrustStoreCertificate	Concede permissão para obter certificados de armazenamentos de trust	Leitura	trustStore*		
GetUserAccessLoggingSettings	Concede permissão para obter detalhes sobre as configurações do usuário	Leitura	userAccessLoggingSettings*		
GetUserSettings	Concede permissão para obter detalhes sobre as configurações do usuário	Leitura	userSettings*		
ListBrowserSettings	Concede permissão para listar configurações do navegador	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListDataProtectionSettings	Concede permissão para listar as configurações de proteção de dados	Leitura			
ListIdentityProviders	Concede permissão para listar provedores de identidade	Leitura	identityProvider*		
ListIpAccessSettings	Concede permissão para listar as configurações de acesso IP	Leitura			
ListNetworkSettings	Concede permissão para listar configurações de rede	Leitura			
ListPortals	Concede permissão para listar portais da web	Leitura			
ListSessionLoggers	Concede permissão para listar registradores de sessão	Leitura			
ListSessions	Concede permissão para listar sessões de um portal usando filtros opcionais	Leitura	portal*		
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Leitura			
ListTrustStoreCertificates	Concede permissão para listar certificados em um armazenamento de trust	Leitura			
ListTrustStores	Concede permissão para listar armazenamento de trust	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListUserAccessLoggingSettings	Concede permissão para listar configurações de registro de acesso	Leitura			
ListUserSettings	Concede permissão para listar configurações de usuário	Leitura			
TagResource	Concede permissão para adicionar uma ou mais etiquetas a um recurso	Marcação	browserSettings		
			dataProtectionSettings		
			identityProvider		
			ipAccessSettings		
			networkSettings		
			portal		
			sessionLogger		
			trustStore		
			userAccessLoggingSettings		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			userSettings		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover uma ou mais etiquetas de um recurso	Tags	browserSettings		
			dataProtectionSettings		
			identityProvider		
			ipAccessSettings		
			networkSettings		
			portal		
			sessionLogger		
			trustStore		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
			userAccessLoggingSettings		
			userSettings		
				aws:TagKeys	
UpdateBrowserSettings	Concede permissão para atualizar configurações do navegador	Gravar	browserSettings*		
UpdateDataProtectionSettings	Concede permissão para atualizar as configurações de proteção de dados	Gravar	dataProtectionSettings*		
UpdateIdentityProvider	Concede permissão para atualizar provedores de identidade	Gravar	identityProvider*		
			portal*		
UpdateIpAccessSettings	Concede permissão para atualizar as configurações de acesso IP	Gravar	ipAccessSettings*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateNetworkSettings	Concede permissão para atualizar configurações de rede	Gravar	networkSettings*		ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateTags ec2:DeleteNetworkInterface ec2:DeleteNetworkInterfacePermission ec2:ModifyNetworkInterfaceAttribute
UpdatePortal	Concede permissão para atualizar um portais da web	Gravar	portal*		
UpdateSessionLogger	Concede permissão para atualizar o registrador de sessão	Gravar	sessionLogger*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateTrustStore	Concede permissão para atualizar armazenamentos de trust	Gravar	trustStore*		
UpdateUserAccessLoggingSettings	Concede permissão para atualizar configurações de registro de acesso	Gravar	userAccessLoggingSettings*		kinesis:PutRecord kinesis:PutRecords
UpdateUserSettings	Concede permissão para atualizar configurações de usuário	Gravar	userSettings*		

Tipos de recursos definidos pelo Amazon WorkSpaces Secure Browser

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
browserSettings	`arn:${Partition}:workspaces-web:${Region}:${Account}:browserSettings/${BrowserSettingsId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
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/${TagKey}
sessionLogger	arn:${Partition}:workspaces-web:${Region}:${Account}:sessionLogger/${SessionLoggerId}	aws:ResourceTag/${TagKey}

Chaves de condição para o Amazon WorkSpaces Secure Browser

O Amazon WorkSpaces Secure Browser define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição para o Amazon WorkSpaces Thin Client

O Amazon WorkSpaces Thin Client (prefixo do serviço:`thinclient`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo Amazon WorkSpaces Thin Client
- Tipos de recursos definidos pelo Amazon WorkSpaces Thin Client
- Chaves de condição para Amazon WorkSpaces Thin Client

Ações definidas pelo Amazon WorkSpaces Thin Client

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de

recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
CreateEnvironment	Concede permissão para criar ambientes	Gravar		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	appstream:DescribeStacks iam:CreateServiceLinkedRole workspaces-web:GetPortal workspaces-web:GetUserSettings workspaces:DescribeWorkspaceDirectories

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteDevice	Concede permissão para excluir dispositivos	Gravar	device*		
				aws:ResourceTag/${TagKey}	
DeleteEnvironment	Concede permissão para excluir ambientes	Gravar	environment*		
				aws:ResourceTag/${TagKey}	
DeregisterDevice	Concede permissão para cancelar o registro de dispositivos	Gravar	device*		
				aws:ResourceTag/${TagKey}	
GetDevice	Concede permissão para obter dispositivos	Leitura	device*		
				aws:ResourceTag/${TagKey}	
GetDeviceDetails [somente permissão]	Concede permissão para obter detalhes de dispositivos	Leitura	device*		
				aws:ResourceTag/${TagKey}	
GetEnvironment	Concede permissão para obter detalhes de ambientes	Leitura	environment*		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
GetSoftwareSet	Concede permissão para obter detalhes de conjuntos de softwares	Leitura	softwareset*		
				aws:ResourceTag/${TagKey}	
ListDeviceSessions [somente permissão]	Concede permissão para listar sessões de dispositivos	Lista	device*		
				aws:ResourceTag/${TagKey}	
ListDevices	Concede permissão para listar dispositivos	Lista			
ListEnvironments	Concede permissão para listar ambientes	Lista			
ListSoftwareSets	Concede permissão para listar conjuntos de softwares	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso	Lista	device		
			environment		
			softwareset		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
TagResource	Concede permissão para adicionar uma ou mais etiquetas a um recurso	Marcação	device		
			environment		
			softwareset		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Concede permissão para remover uma ou mais etiquetas de um recurso	Tags	device		
			environment		
			softwareset		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateDevice	Concede permissão para atualizar dispositivos	Gravar	device*		
				aws:ResourceTag/${TagKey}	
UpdateEnvironment	Concede permissão para atualizar ambientes	Gravar	environment*		appstream:DescribeStacks workspaces-web:GetPortal workspaces-web:GetUserSettings workspaces:DescribeWorkspaceDirectories

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:ResourceTag/${TagKey}	
UpdateSoftwareSet	Concede permissão para atualizar conjuntos de softwares	Gravar	softwareset*		
				aws:ResourceTag/${TagKey}	

Tipos de recursos definidos pelo Amazon WorkSpaces Thin Client

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
environment	`arn:${Partition}:thinclient:${Region}:${Account}:environment/${EnvironmentId}`	aws:ResourceTag/${TagKey}
device	`arn:${Partition}:thinclient:${Region}:${Account}:device/${DeviceId}`	aws:ResourceTag/${TagKey}

Tipos de recursos	ARN	Chaves de condição
softwareset	`arn:${Partition}:thinclient:${Region}:${Account}:softwareset/${SoftwareSetId}`	aws:ResourceTag/${TagKey}

Chaves de condição para Amazon WorkSpaces Thin Client

O Amazon WorkSpaces Thin Client define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString

Ações, recursos e chaves de condição do AWS X-Ray

AWS O X-Ray (prefixo do serviço:`xray`) fornece os seguintes recursos, ações e chaves de contexto de condição específicos do serviço para uso nas políticas de permissão do IAM.

Referências:

- Saiba como configurar este serviço.
- Visualize uma lista das operações de API disponíveis para este serviço.
- Saiba como proteger esse serviço e seus recursos usando políticas de permissão do IAM.

Tópicos

- Ações definidas pelo AWS X-Ray
- Tipos de recursos definidos pelo AWS X-Ray
- Chaves de condição do AWS X-Ray

Ações definidas pelo AWS X-Ray

Você pode especificar as seguintes ações no elemento `Action` de uma declaração de política do IAM. Use políticas para conceder permissões para executar uma operação na AWS. Quando usa uma ação em uma política, você geralmente permite ou nega acesso à operação da API ou ao comando da CLI com o mesmo nome. No entanto, em alguns casos, uma única ação controla o acesso a mais de uma operação. Como alternativa, algumas operações exigem várias ações diferentes.

A coluna Nível de acesso da tabela Ações descreve como a ação é classificada (Lista, Leitura, Gerenciamento de permissões ou Marcação). Esta classificação pode ajudar você a compreender o nível de acesso que uma ação concede quando a usa em uma política. Para obter mais informações sobre os níveis de acesso, consulte Níveis de acesso nos resumos das políticas.

A coluna Tipos de recursos na tabela Ações indica se cada ação é compatível com permissões no nível do recurso. Se não houver valor para essa coluna, você deverá especificar todos os recursos ("*") aos quais a política se aplica no elemento `Resource` de sua declaração de política. Se a coluna incluir um tipo de recurso, você poderá especificar um ARN desse tipo em uma instrução com essa ação. Se a ação tiver um ou mais recursos necessários, o chamador deverá ter permissão para usar a ação com esses recursos. Os recursos obrigatórios são indicados na tabela com um asterisco (*). Se você limitar o acesso aos recursos com o elemento `Resource` em uma política do IAM, deverá incluir um ARN ou padrão para cada tipo de recurso necessário. Algumas ações oferecem suporte a vários tipos de recursos. Se o tipo de recurso for opcional (não indicado como obrigatório), você poderá optar por usar um dos tipos de recurso opcionais.

A coluna Chaves de condição na tabela Ações inclui chaves que você pode especificar em um elemento `Condition` da declaração de política. Para obter mais informações sobre as chaves de

condição associadas aos recursos do serviço, consulte a coluna Chaves de condição da tabela Tipos de recursos.

> **Note**
>
> As chaves de condição do recurso estão listadas na tabela Tipos de recursos. Você pode encontrar um link para o tipo de recurso que se aplica a uma ação na coluna Tipos de recursos (*obrigatório) da tabela Ações. O tipo de recurso na tabela Tipos de recursos inclui a coluna Chaves de condição, que são as chaves de condição do recurso que se aplicam a uma ação na tabela Ações.

Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de ações.

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
BatchGetTraceSummaryById [somente permissão]	Concede permissão para recuperar metadados de uma lista de rastreamentos especificados por ID	Leitura			
BatchGetTraces	Concede permissão para recuperar uma lista de rastreamentos especificados por ID. Cada rastreamento é uma coleção de documentos de segmentos originários de uma única solicitação. Use GetTraceSummaries para obter uma lista de traços IDs	Lista			
CancelTraceRetrieval	Concede permissão para cancelar um trabalho de recuperação de rastreame	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
	nto em andamento iniciado StartTraceRetrieval usando o fornecido RetrievalToken. Um cancelamento bem-sucedido retornará uma resposta HTTP 200				
CreateGroup	Concede permissão para criar um recurso de grupo com um nome e uma expressão de filtro	Write	group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSamplingRule	Concede permissão para criar uma regra para controlar o comportamento de amostragem para aplicações instrumentadas	Write	sampling-rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteGroup	Concede permissão para excluir um recurso de grupo	Gravar	group*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
DeleteResourcePolicy	Concede permissão para excluir políticas de recurso	Gravar		xray:ResourcePolicyName	
DeleteSamplingRule	Concede permissão para excluir uma regra de amostragem	Gravar	sampling-rule*		
				aws:ResourceTag/${TagKey}	
GetDistinctTraceGraphs [somente permissão]	Concede permissão para recuperar gráficos de serviços distintos para um ou mais rastreamentos específicos IDs	Leitura			
GetEncryptionConfig	Concede permissão para recuperar a configuração atual de criptografia para dados do X-Ray	Read			
GetGroup	Concede permissão para recuperar detalhes do recurso do grupo	Read	group*		
				aws:ResourceTag/${TagKey}	
GetGroups	Concede permissão para recuperar os detalhes de todos os grupos ativos	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetIndexingRules	Concede permissão para recuperar todas as regras de indexação. As regras de indexação são usadas para determinar a taxa de amostragem do lado do servidor para extensões ingeridas pelo destino e indexadas pelo X-Ray CloudWatchLogs	Leitura			
GetInsight	Concede permissão para recuperar os detalhes de um insight específico	Read			
GetInsightEvents	Concede permissão para recuperar os eventos de um insight específico	Read			
GetInsightImpactGraph	Concede permissão para recuperar a parte do gráfico de serviço que é afetada por um insight específico	Read			
GetInsightSummaries	Concede permissão para recuperar o resumo de todos os insights de um grupo e intervalo de tempo com filtros opcionais	Leitura			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetRetrievedTracesGraph	Concede permissão para recuperar um gráfico de serviço para rastreamentos com base no especificado do grupo RetrievalToken de CloudWatch registros de Pesquisa de Transações	Leitura			
GetSamplingRules	Concede permissão para recuperar todas as regras de amostragem	Read			
GetSamplingStatisticSummaries	Concede permissão para recuperar informações sobre resultados de amostragem recentes para todas as regras de amostragem	Read			
GetSamplingTargets	Concede permissão para solicitar uma cota de amostragem para regras que o serviço está usando para solicitações de amostra	Read			
GetServiceGraph	Concede permissão para recuperar um documento que descreve os serviços que processam solicitações de entrada e serviços downstream que elas chamam como um resultado	Read			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
GetTimeSeriesServiceStatistics	Concede permissão para recuperar uma agregação de estatísticas de serviço definida por um período específico dividido em buckets de intervalos de tempo.	Leitura			
GetTraceGraph	Concede permissão para recuperar um gráfico de serviço para um ou mais rastreamentos específicos IDs	Leitura			
GetTraceSegmentDestination	Concede permissão para recuperar o destino atual dos dados enviados para uma PutTraceSegments API OpenTelemetry	Leitura			
GetTraceSummaries	Concede permissão para recuperar IDs e metadados para rastreamentos disponíveis por um período de tempo especificado usando um filtro opcional. Para obter os traços completos, passe o rastreamento IDs para BatchGetTraces	Leitura			
Link [somente permissão]	Concede permissão para compartilhar recursos do X-Ray com uma conta de monitoramento	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
ListResourcePolicies	Concede permissão para listar políticas de recurso	Lista			
ListRetrievedTraces	Concede permissão para recuperar uma lista de rastreamentos de um determinado RetrievalToken do grupo de CloudWatch registros de Pesquisa de Transações	Lista			
ListTagsForResource	Concede permissão para listar as etiquetas de um recurso do X-Ray	List	group		
			sampling-rule		
PutEncryptionConfig	Concede permissão para atualizar a configuração de criptografia para dados do X-Ray	Gerenciamento de permissões			
PutResourcePolicy	Concede permissão para criar ou atualizar políticas de recurso	Gravar		xray:ResourcePolicyName	
PutSpans	Concede permissão para fazer upload de extensões OpenTelemetry para o X-Ray AWS	Gravar			

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
PutSpansForIndexing [somente permissão]	Concede permissão para fazer upload de extensões para o AWS X-Ray para serem indexadas	Gravar			
PutTelemetryRecords	Concede permissão para enviar a telemetria do daemon AWS X-Ray para o serviço	Gravar			
PutTraceSegments	Concede permissão para fazer upload de documentos do segmento para o AWS X-Ray. O SDK do X-Ray gera documentos de segmento e os envia ao daemon do X-Ray, que faz upload deles em lotes.	Gravar			
StartTraceRetrieval	Concede permissão para iniciar um processo de recuperação de rastreamento usando o intervalo de tempo especificado e para o rastreamento fornecido IDs no grupo de registros de Pesquisa CloudWatch de Transações	Leitura			
TagResource	Concede permissão para adicionar etiquetas a um recurso do X-Ray.	Marcação	group sampling-rule		

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Concede permissão para remover etiquetas de um recurso do X-Ray.	Marcação	group		
			sampling-rule		
				aws:TagKeys	
UpdateGroup	Concede permissão para atualizar um recurso de grupo.	Gravar	group*		
				aws:ResourceTag/${TagKey}	
UpdateIndexingRule	Concede permissão para modificar a configuração de uma regra de indexação	Gravar			
UpdateSamplingRule	Concede permissão para modificar a configuração de uma regra de amostragem	Gravar	sampling-rule*		
				aws:ResourceTag/${TagKey}	

Ações	Descrição	Nível de acesso	Tipos de recursos (*necessários)	Chaves de condição	Ações dependentes
UpdateTraceSegmentDestination	Concede permissão para modificar o destino dos dados enviados para PutTraceSegments uma OpenTelemetry API	Gravar		xray:TraceSegmentDestination	

Tipos de recursos definidos pelo AWS X-Ray

Os seguintes tipos de recursos são definidos por este serviço e podem ser usados no elemento `Resource` de declarações de políticas de permissão do IAM. Cada ação na Tabela de ações identifica os tipos de recursos que podem ser especificados com essa ação. Um tipo de recurso também pode definir quais chaves de condição você pode incluir em uma política. Essas chaves são exibidas na última coluna da tabela Tipos de recursos. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de tipos de recursos.

Tipos de recursos	ARN	Chaves de condição
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}

Chaves de condição do AWS X-Ray

AWS O X-Ray define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre as colunas na tabela a seguir, consulte Tabela de chaves de condição.

Para ver as chaves de condição globais que estão disponíveis para todos os serviços, consulte chaves de contexto de condição AWS global.

Chaves de condição	Descrição	Tipo
aws:RequestTag/${TagKey}	Filtra o acesso pelas etiquetas que são transmitidas na solicitação	Segmento
aws:ResourceTag/${TagKey}	Filtra o acesso pelas etiquetas associadas ao recurso	Segmento
aws:TagKeys	Filtra o acesso pelas chaves da etiqueta que são transmitidas na solicitação	ArrayOfString
xray:ResourcePolicyName	Filtra o acesso por PolicyName na solicitação	String
xray:TraceSegmentDestination	Filtra o acesso por TraceSegmentDestination tipo na solicitação	String

Recursos relacionados

Para obter as informações relacionadas no Guia do usuário do IAM, consulte os seguintes recursos:

- Tutorial: crie e anexe a sua primeira política gerenciada pelo cliente
- AWS serviços que funcionam com o IAM
- Lógica da avaliação de política

AWS service (Serviço da AWS) Informações simplificadas para acesso programático

AWS fornece informações de referência de serviços no formato JSON para agilizar a automação dos fluxos de trabalho de gerenciamento de políticas. Com as informações de referência do serviço, você pode acessar as ações, os recursos e as chaves Serviços da AWS de condição disponíveis em arquivos legíveis por máquina. As informações de referência do serviço incluem metadados além dos detalhes da autorização, incluindo informações sobre o último acesso da ação do IAM e dados de geração de políticas do IAM Access Analyzer.

Os administradores de segurança podem estabelecer barreiras e os desenvolvedores podem garantir o acesso adequado aos aplicativos identificando as ações, os recursos e as chaves de condição disponíveis para cada um. AWS service (Serviço da AWS) AWS fornece informações de referência do serviço Serviços da AWS para permitir que você incorpore os metadados em seus fluxos de trabalho de gerenciamento de políticas.

- Para obter um inventário de ações, recursos e chaves de condição para uso nas políticas do IAM, consulte a página de referência de autorização de serviço para AWS service (Serviço da AWS) o. Ações, recursos e chaves de condição para serviços que compartilham um prefixo de serviço podem ser divididos em várias páginas na Referência de Autorização de Serviço.
- Para ver uma lista das ações Serviços da AWS e das ações para as quais as informações acessadas pela última ação do IAM são exibidas, consulte Serviços e ações de informações acessadas pela última ação do IAM no Guia do usuário do IAM.
- Para ver uma lista de ações Serviços da AWS e ações para as quais o IAM Access Analyzer gera políticas com informações em nível de ação, consulte Serviços de geração de políticas do IAM Access Analyzer no Guia do usuário do IAM.

O conteúdo apresentado na Referência de Autorização de Serviço pode ser apresentado de forma diferente ou conter metadados diferentes. Para obter mais informações, consulte Definições de campo adicionais.

> **Note**
>
> As alterações nas informações de referência do serviço podem levar até 24 horas para serem refletidas na lista de metadados do serviço.

Acessando informações AWS service (Serviço da AWS) de referência

1. Navegue até as informações de referência do serviço para acessar a lista Serviços da AWS para as quais as informações de referência estão disponíveis.

   O exemplo a seguir mostra uma lista parcial de serviços e URLs suas respectivas informações de referência:

   ```
   [
       {
           "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. Escolha um serviço e navegue até a página de informações do serviço no `url` campo do serviço para ver uma lista de ações, recursos e chaves de condição do serviço.

   O exemplo a seguir mostra uma lista parcial de informações de referência de serviços para o Amazon S3:

   ```
   {
       "Name": "s3",
       "Actions": [
           {
               "Name": "GetObject",
               "ActionConditionKeys": [
                   "s3:AccessGrantsInstanceArn",
                   "s3:AccessPointNetworkOrigin",
   ```

```
                "s3:DataAccessPointAccount",
                "s3:DataAccessPointArn",
                "s3:ExistingObjectTag/key",
                "s3:ResourceAccount",
                "s3:TlsVersion",
                "s3:authType",
                "s3:if-match",
                "s3:if-none-match",
                "s3:signatureAge",
                "s3:signatureversion",
                "s3:x-amz-content-sha256"
            ],
            "Annotations" : {
                "Properties" : {
                    "IsList" : false,
                    "IsPermissionManagement" : false,
                    "IsTaggingOnly" : false,
                    "IsWrite" : false
                }
            },
            "Resources": [
                {
                    "Name": "object"
                }
            ],
            "SupportedBy" : {
                "IAM Access Analyzer Policy Generation" : false,
                "IAM Action Last Accessed" : false
            }
        },
        {
            "Name": "ListBucket",
            "ActionConditionKeys": [
                "s3:AccessGrantsInstanceArn",
                "s3:AccessPointNetworkOrigin",
                "s3:DataAccessPointAccount",
                "s3:DataAccessPointArn",
                "s3:ResourceAccount",
                "s3:TlsVersion",
                "s3:authType",
                "s3:delimiter",
                "s3:max-keys",
                "s3:prefix",
                "s3:signatureAge",
```

```
                "s3:signatureversion",
                "s3:x-amz-content-sha256"
            ],
            "Annotations" : {
                "Properties" : {
                    "IsList" : true,
                    "IsPermissionManagement" : false,
                    "IsTaggingOnly" : false,
                    "IsWrite" : false
                }
            },
            "Resources": [
                {
                    "Name": "bucket"
                }
            ],
            "SupportedBy" : {
                "IAM Access Analyzer Policy Generation" : false,
                "IAM Action Last Accessed" : false
            }
        },
        ...
    ],
    "ConditionKeys": [
        {
            "Name": "s3:TlsVersion",
            "Types": [
                "Numeric"
            ]
        },
        {
            "Name": "s3:authType",
            "Types": [
                "String"
            ]
        },
        ...
    ],
    "Resources": [
        {
            "Name": "accesspoint",
            "ARNFormats": [
                "arn:${Partition}:s3:${Region}:${Account}:accesspoint/
${AccessPointName}"
```

```
            ]
        },
        {
            "Name": "bucket",
            "ARNFormats": [
                "arn:${Partition}:s3:::${BucketName}"
            ]
        }
        ...
    ],
    "Version": "v1.3"
}
```

3. Baixe o arquivo JSON do URL do serviço para usar em seus fluxos de trabalho de criação de políticas.

Definições de campo adicionais

As propriedades da ação fornecem metadados adicionais sobre as ações de serviço para ajudar a categorizá-las com base no escopo da permissão. Essas propriedades são encontradas no `Annotations` campo de cada ação. Os metadados consistem em quatro valores booleanos:

- `IsList`— Fornece permissões para descobrir e listar recursos, incluindo metadados básicos, sem acessar o conteúdo dos recursos.

  Exemplo — Essa propriedade é `true` para a `ListBucket` ação do Amazon S3, permitindo que os usuários visualizem listas de buckets sem acessar os próprios objetos.

- `IsPermissionManagement`— Fornece permissões para modificar as permissões do IAM ou as credenciais de acesso.

  Exemplo — Essa propriedade é `true` para a maioria das AWS Organizations ações e do IAM, bem como para ações do Amazon S3, como e. `PutBucketPolicy` `DeleteBucketPolicy`

- `IsTaggingOnly`— Fornece permissões somente para modificar tags.

  Exemplo — Essa propriedade é `true` para ações do IAM `TagRole` e`UntagRole`, embora seja `false` para, ela `CreateRole` fornece permissões mais amplas além da marcação.

- `IsWrite`— Fornece permissões para modificar recursos, o que pode incluir modificações de tags.

Exemplo — Essa propriedade é `true` para ações do Amazon S3 e `CreateBucketDeleteBucket`, `PutObject` pois elas permitem a modificação de recursos.

> **Note**
>
> Essas propriedades não são mutuamente exclusivas. Uma ação pode ter várias propriedades definidas como`true`.
> Também é possível que todas as propriedades sejam`false`, como visto com a ação do `GetObject` Amazon S3. Isso indica que a ação só concede permissões de leitura em um objeto.

Essas propriedades podem ser usadas para gerar insights sobre serviços. O exemplo a seguir mostra quais permissões com o `s3` prefixo permitem a mutação de 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"
...
```

O exemplo a seguir mostra quais chaves de condição de ação com o `lambda` prefixo você pode usar para limitar o acesso às ações de gerenciamento de permissões:

```
> 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"
    ]
}
```

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.