亚马逊云科技

服务授权参考

服务授权参考

服务授权参考: 服务授权参考

Amazon Web Services 文档中描述的 Amazon Web Services 服务或功能可能因区域而异。要查看适用于中国区域的差异，请参阅 中国的 Amazon Web Services 服务入门 (PDF)。

Table of Contents

参考

《服务授权参考》提供了每项 Amazon 服务支持的操作、资源和条件键的列表。您可以在 Amazon Identity and Access Management (IAM) 策略中指定操作、资源和条件密钥来管理对 Amazon 资源的访问权限。

内容

Amazon 服务的操作、资源和条件键

每项 Amazon 服务都可以定义在 IAM 策略中使用的操作、资源和条件上下文密钥。本主题介绍如何记录为每项服务提供的元素。

每个主题由各个表组成，而表提供可用操作、资源和条件键的列表。

操作表

操作表列出所有可以在 IAM policy语句的 `Action` 元素中使用的操作。并非服务定义的所有 API 操作都可以用作 IAM policy 中的操作。某些服务包括与 API 操作不直接对应的仅限权限的操作。这些操作以 [仅限权限] 表示。使用此列表可确定哪些操作可用于 IAM policy 中。有关 `Action`、`Resource` 或 `Condition` 元素的更多信息，请参阅 IAM JSON 策略元素参考。操作和描述表列是自描述性的。

- 访问级别列描述如何对操作进行分类（列出、读取、写入、权限管理或标记）。此分类可以帮助您了解当您在策略中使用操作时，相应操作授予的访问级别。有关访问级别的更多信息，请参阅了解策略摘要内的访问级别摘要。
- 资源类型列指示操作是否支持资源级权限。如果该列为空，则操作不支持资源级权限，并且您必须在策略中指定所有资源（“*”）。如果该列包含一种资源类型，则可以在策略的 `Resource` 元素中指定资源 ARN。有关资源的更多信息，请参阅资源类型表中相应的行。一个语句中包括的所有操作和资源必须相互兼容。如果您指定的资源对操作无效，则任何使用该操作的请求都会失败，并且语句的 `Effect` 不适用。

  必需资源在表中以星号 (*) 表示。如果在使用该操作的语句中指定资源级权限 ARN，则它必须属于该类型。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种类型而不使用其他类型。

- 条件键列包括可以在策略语句的 Condition 元素中指定的键。可能支持将条件键与操作或操作和特定资源一起使用。请密切注意该键是否与特定资源类型位于同一行中。该表不包括适用于任何操作或不相关情况的全局条件键。有关全局条件键的更多信息，请参阅Amazon 全局条件上下文键。
- 除了操作本身的权限以外，相关操作列还包括成功调用该操作所应该具有的任何其他权限。如果操作访问多个资源，这可能是必需的。

  并非在所有情况下都需要相关操作。有关为用户提供精细权限的更多信息，请参阅各个服务的文档。

资源类型表

资源类型表列出您可以在 Resource 策略元素中指定为 ARN 的所有资源类型。并非可以为每个操作指定每种资源类型。某些资源类型仅适用于某些操作。如果在语句中指定一种资源类型并且操作不支持该资源类型，则该语句不允许访问。有关 Resource 元素的更多信息，请参阅 IAM JSON 策略元素：Resource。

- ARN 列指定，在引用该类型的资源时必须使用的 Amazon Resource Name (ARN) 格式。前缀为 $ 的部分必须替换为您的方案的实际值。例如，如果在 ARN 中看到 $user-name，您必须将该字符串替换为实际用户的名称或包含用户名的策略变量。有关的更多信息 ARNs，请参阅 IAM ARNs。
- 条件键列指定条件上下文键，只有在 IAM policy 语句中同时包含该资源和上表中的支持操作时，才能在该语句中包含这些键。

条件键表

条件键表列出可以在 IAM policy 语句的 Condition 元素中使用的所有条件上下文键。并非可以对每个操作或资源指定每个键。某些键仅适用于特定类型的操作和资源。有关 Condition 元素的更多信息，请参阅 IAM JSON 策略元素：Condition。

- 类型列指定条件键的数据类型。该数据类型确定您可以使用哪些条件运算符以将请求中的值与策略语句中的值进行比较。您必须使用一个适用于数据类型的运算符。如果您使用不正确的运算符，匹配始终会失败，而策略语句从不适用。

  如果 Type (类型) 列指定某种简单类型“...列表”，则可以在策略中使用多个键和值。使用条件集前缀以及运算符执行此操作。使用 ForAllValues 前缀指定请求中的所有值必须与策略语句中的值匹配。使用 ForAnyValue 前缀指定请求中至少有一个值与策略语句中的其中一个值匹配。

主题

- Amazon 账户管理的操作、资源和条件键
- 适用于 APIs 亚马逊 MSK 集群的 Apache Kafka 的操作、资源和条件密钥
- Amazon API Gateway 的操作、资源和条件键
- Amazon App Mesh 的操作、资源和条件键
- Amazon AppConfig 的操作、资源和条件键
- Amazon Application Auto Scaling 的操作、资源和条件键
- Amazon 应用程序恢复控制器的操作、资源和条件键-Zonal Shift
- Amazon AppSync 的操作、资源和条件键
- Amazon Athena 的操作、资源和条件键
- Amazon Backup 的操作、资源和条件键
- Amazon Backup Gateway 的操作、资源和条件键
- Amazon Backup 存储的操作、资源和条件键
- Amazon Batch 的操作、资源和条件键
- Amazon Billing的操作、资源和条件键
- Amazon Billing 控制台的操作、资源和条件键
- Amazon Budget Service 的操作、资源和条件键
- Amazon Certificate Manager 的操作、资源和条件键
- Amazon Web Services 云 Map 的操作、资源和条件键
- Amazon CloudAssist 服务读写权限的操作、资源和条件密钥
- Amazon CloudFormation 的操作、资源和条件键
- Amazon 的操作、资源和条件密钥 CloudFront
- Amazon CloudTrail 的操作、资源和条件键
- Amazon 的操作、资源和条件密钥 CloudWatch
- Amazon App CloudWatch lication Insights 的操作、资源和条件键
- Amazon CloudWatch 日志的操作、资源和条件密钥
- Amazon CloudWatch 可观察性访问管理器的操作、资源和条件密钥
- Amazon Sy CloudWatch nthetics 的操作、资源和条件密钥
- Amazon CodeBuild 的操作、资源和条件键
- Amazon CodeCommit 的操作、资源和条件键

- Amazon CodeDeploy 的操作、资源和条件键
- Amazon CodeDeploy 安全主机命令服务的操作、资源和条件密钥
- Amazon CodePipeline 的操作、资源和条件键
- Amazon Cognito Identity 的操作、资源和条件键
- Amazon Compute Optimizer 的操作、资源和条件键
- Amazon Config 的操作、资源和条件键
- Amazon Connector Service 的操作、资源和条件键
- Amazon 整合账单的操作、资源和条件键
- Amazon 成本和使用情况报告的操作、资源和条件键
- Amazon Cost Explorer Service 的操作、资源和条件键
- Amazon Data Lifecycle Manager 的操作、资源和条件键
- Amazon Database Migration Service 的操作、资源和条件键
- Amazon Direct Connect 的操作、资源和条件键
- Amazon Directory Service 的操作、资源和条件键
- Amazon DynamoDB 的操作、资源和条件键
- Amazon DynamoDB Accelerator (DAX) 的操作、资源和条件键
- Amazon A EC2 uto Scaling 的操作、资源和条件密钥
- Amazon EC2 Image Builder 的操作、资源和条件密钥
- Amazon EC2 Instance Connect 的操作、资源和条件密钥
- Amazon EKS Auth 的操作、资源和条件键
- Amazon Elastic Beanstalk 的操作、资源和条件键
- Amazon Elastic Block Store 的操作、资源和条件键
- Amazon Elastic Container Registry 的操作、资源和条件键
- Amazon Elastic File System 的操作、资源和条件键
- Amazon Elastic Kubernetes Service 的操作、资源和条件键
- Amazon Elastic Load Balancing 的操作、资源和条件键
- Amazon Elastic Load Balancing V2 的操作、资源和条件键
- Amazon Elastic 的操作、资源和条件密钥 MapReduce
- Amazon 的操作、资源和条件密钥 ElastiCache
- Amazon 元素的动作、资源和条件键 MediaConvert

- Amazon EMR Serverless 的操作、资源和条件键
- Amazon 的操作、资源和条件密钥 EventBridge
- Amazon 发票管理的操作、资源和条件键
- Amazon 免费套餐的操作、资源和条件键
- Amazon FreeRTOS 的操作、资源和条件键
- Amazon 的操作、资源和条件密钥 FSx
- Amazon 的操作、资源和条件密钥 GameLift
- Amazon Glue 的操作、资源和条件键
- Glue 的操作、资源和条件 Amazon 键 DataBrew
- Amazon 的操作、资源和条件密钥 GuardDuty
- Healt Amazon h 和 Notifications 的操作、资源 APIs 和条件键
- Amazon IAM Access Analyzer 的操作、资源和条件键
- Amazon IAM 身份中心（ Amazon 单点登录的继任者）的操作、资源和条件密钥
- Amazon IAM Identity Center（ Amazon 单点登录的继任者）目录的操作、资源和条件密钥
- Amazon IAM Identity Center OIDC 服务的操作、资源和条件键
- Amazon Identity and Access Management（IAM）的操作、资源和条件键
- Amazon Identity And Access Management 的操作、资源和条件键
- Amazon Identity Store 的操作、资源和条件键
- Amazon Identity Store Auth 的操作、资源和条件键
- Amazon Identity Sync 的操作、资源和条件键
- Amazon Inspector2 的操作、资源和条件键
- Amazon Invoicing Service 的操作、资源和条件键
- Amazon IoT Analytics 的操作、资源和条件键
- Amazon IoT Events 的操作、资源和条件键
- Amazon IoT Greengrass 的操作、资源和条件键
- Amazon IoT Greengrass V2 的操作、资源和条件键
- Amazon 物联网任务的操作、资源和条件键 DataPlane
- Amazon 物联网的操作、资源和条件键 SiteWise
- Amazon 物联网的操作、资源和条件键 TwinMaker
- Amazon Kinesis Analytics 的操作、资源和条件键

- Amazon Kinesis Analytics V2 的操作、资源和条件键
- Amazon Kinesis Data Streams 的操作、资源和条件键
- Amazon Kinesis Firehose 的操作、资源和条件键
- Amazon Kinesis Video Streams 的操作、资源和条件键
- Amazon Lambda 的操作、资源和条件键
- Amazon Launch Wizard 的操作、资源和条件键
- Amazon License Manager 的操作、资源和条件键
- Amazon License Manager Linux Subscriptions Manager 的操作、资源和条件键
- Amazon Managed Streaming for Apache Kafka 的操作、资源和条件键
- Amazon Managed Workflows for Apache Airflow 的操作、资源和条件键
- Amazon Web Services Marketplace的操作、资源和条件键
- Amazon Web Services Marketplace Entitlement Service 的操作、资源和条件键
- Amazon Web Services Marketplace Management Portal 的操作、资源和条件键
- Amazon Web Services Marketplace Metering Service 的操作、资源和条件键
- Amazon MemoryDB 的操作、资源和条件密钥
- Amazon Message Delivery Service 的操作、资源和条件键
- Amazon Message Gateway Service 的操作、资源和条件键
- Amazon MQ 的操作、资源和条件键
- Amazon Neptune 的操作、资源和条件键
- Amazon Network Firewall 的操作、资源和条件键
- Amazon OpenSearch 服务的操作、资源和条件密钥
- Amazon Organizations 的操作、资源和条件键
- Amazon Payments 的操作、资源和条件键
- Amazon Performance Insights 的操作、资源和条件键
- Amazon Personalize 的操作、资源和条件键
- Amazon Polly 的操作、资源和条件键
- Amazon Price List 的操作、资源和条件键
- Amazon Private Certificate Authority 的操作、资源和条件键
- Amazon 采购订单控制台的操作、资源和条件键
- Amazon 的操作、资源和条件密钥 QuickSight

- Amazon RDS IAM Authentication 的操作、资源和条件键
- 适用于 Amazon Recycle Bin 的操作、资源和条件键
- Amazon Redshift 的操作、资源和条件键
- Amazon Redshift Data API 的操作、资源和条件键
- Amazon Redshift Serverless 的操作、资源和条件键
- Amazon Resource Access Manager（RAM）的操作、资源和条件键
- Amazon Resource Group Tagging API 的操作、资源和条件键
- Amazon Resource Groups 的操作、资源和条件键
- Amazon Route 53 的操作、资源和条件键
- Amazon Route 53 Resolver 的操作、资源和条件键
- Amazon S3 Glacier 的操作、资源和条件键
- Amazon S3 Object Lambda 的操作、资源和条件键
- Amazon Savings Plans 的操作、资源和条件键
- Amazon Secrets Manager 的操作、资源和条件键
- Amazon Security Hub 的操作、资源和条件键
- Amazon Server Migration Service 的操作、资源和条件键
- Amazon Serverless Application Repository 的操作、资源和条件键
- Service Quotas 的操作、资源和条件键
- Amazon Signer 的操作、资源和条件键
- Amazon Simple Workflow Service 的操作、资源和条件键
- Amazon SimpleDB 的操作、资源和条件键
- Amazon Snowball 的操作、资源和条件键
- Amazon SNS 的操作、资源和条件键
- Amazon SQL Workbench 的操作、资源和条件键
- Amazon SQS 的操作、资源和条件键
- Amazon Step Functions 的操作、资源和条件键
- Amazon Storage Gateway 的操作、资源和条件键
- Amazon Web Services 支持的操作、资源和条件键
- Amazon Systems Manager 的操作、资源和条件键
- Amazon Systems Manager GUI Connect 的操作、资源和条件键

- Amazon Timestream InfluxDB 的操作、资源和条件键
- Amazon Transcribe 的操作、资源和条件键
- Amazon Transfer Family 的操作、资源和条件键
- Amazon Trusted Advisor 的操作、资源和条件键
- Amazon WAF Regional 的操作、资源和条件键
- Amazon WAF V2 的操作、资源和条件键
- Amazon 的操作、资源和条件密钥 WorkSpaces
- Amazon X-Ray 的操作、资源和条件键

Amazon 账户管理的操作、资源和条件键

Amazon 账户管理（服务前缀:account）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon 账户管理定义的操作
- Amazon 账户管理定义的资源类型
- Amazon 账户管理的条件键

Amazon 账户管理定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须

具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AcceptPrimaryEmailUpdate	授予权限以接受账户的主电子邮件地址的更新流程	写入	accountInOrganization		
				account:EmailTargetDomain	
CloseAccount[仅权限]	授予关闭账户的权限	写入	account		
DeleteAlternateContact	授予权限以删除账户的备用联系人	写入	account		
			accountInOrganization		
				account:AlternateC	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				ontactTypes	
DisableRegion	授予权限以禁用使用区域	写入	account		
			accountInOrganization		
				account:TargetRegion	
EnableRegion	授予权限以启用使用区域	写入	account		
			accountInOrganization		
				account:TargetRegion	
GetAccountInformation[仅权限]	授予检索账户信息的权限	读取	account		
GetAlternateContact	授予权限以检索账户的备用联系人	读取	account		
			accountInOrganization		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				account:AlternateContactTypes	
GetContactInformation	授予权限以检索账户的主要联系人信息	读取	account		
			accountInOrganization		
GetPrimaryEmail	授予权限以检索账户的主电子邮件地址	读取	accountInOrganization		
GetRegionOptStatus	授予获取区域的加入状态的权限	读取	account		
			accountInOrganization		
				account:TargetRegion	
ListRegions	授予权限以列出可用区域	列表	account		
			accountInOrganization		
PutAlternateContact	授予权限以修改账户的备用联系人	写入	account		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			accountInOrganization		
				account:AlternateContactTypes	
PutContactInformation	授予权限以更新账户的主要联系人信息	写入	account		
			accountInOrganization		
StartPrimaryEmailUpdate	授予权限以启动账户的主电子邮件地址的更新流程	写入	accountInOrganization		
				account:EmailTargetDomain	

Amazon 账户管理定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
account	arn:${Partition}:account::${Account}:account	
accountInOrganization	arn:${Partition}:account::${ManagementAccountId}:account/o-${OrganizationId}/${MemberAccountId}	

Amazon 账户管理的条件键

Amazon 账户管理定义了可在 IAM 策略Condition元素中使用的以下条件密钥。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
account:AccountResourceOrgPaths	按企业中账户的资源路径筛选访问	ArrayOfString
account:AccountResourceOrgTags/${TagKey}	按企业中账户的资源标签筛选访问	字符串
account:AlternateContactTypes	按备用联系人类型筛选访问	ArrayOfString
account:EmailTargetDomain	按目标电子邮件地址的电子邮件域筛选访问权限	字符串
account:TargetRegion	按区域列表筛选访问。启用或禁用此处指定的所有区域	字符串

适用于 APIs 亚马逊 MSK 集群的 Apache Kafka 的操作、资源和条件密钥

Apache Kafka for A APIs mazon MSK 集群（服务前缀:`kafka-cluster`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Apache Kafka 为 APIs 亚马逊 MSK 集群定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AlterCluster	授予更改集群各个方面的权限，相当于 Apache Kafka 的 ALTER CLUSTER ACL	Write	cluster*		kafka-cluster:Connect kafka-cluster:DescribeCluster
AlterClusterDynamicConfiguration	授予更改集群动态配置的权限，相当于 Apache Kafka 的 ALTER_CONFIGS CLUSTER ACL	Write	cluster*		kafka-cluster:Connect kafka-cluster:DescribeClusterDynamicConfiguration
AlterGroup	授予加入集群上群组的权限，相当于 Apache Kafka 的 READ GROUP ACL	Write	group*		kafka-cluster:Connect kafka-cluster:DescribeGroup
AlterTopic	授予更改集群上主题的权限，相当于 Apache Kafka 的 ALTER TOPIC ACL	Write	topic*		kafka-cluster:Connect

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
					kafka-cluster:DescribeTopic
AlterTopicDynamicConfiguration	授予更改集群上主题的动态配置的权限，相当于 Apache Kafka 的 ALTER_CONFIGS TOPIC ACL	写入	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopicDynamicConfiguration
AlterTransactionalId	授予修改集群 IDs 上事务的权限，相当于 Apache Kafka 的 WRITE TRANSACTIONAL_ID ACL	写入	transactional-id*		kafka-cluster:Connect kafka-cluster:DescribeTransactionalId kafka-cluster:WriteData
Connect	授予连接和验证集群的权限	Write	cluster*		
CreateTopic	授予在集群上创建主题的权限，相当于 Apache Kafka 的 CREATE CLUSTER/TOPIC ACL	Write	topic*		kafka-cluster:Connect

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteGroup	授予删除集群上的群组的权限，相当于 Apache Kafka 的 DELETE GROUP ACL	Write	group*		kafka-cluster:Connect kafka-cluster:DescribeGroup
DeleteTopic	授予删除集群上主题的权限，相当于 Apache Kafka 的 DELETE TOPIC ACL	Write	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopic
DescribeCluster	授予描述集群各个方面的权限，相当于 Apache Kafka 的 DESCRIBE CLUSTER ACL	List	cluster*		kafka-cluster:Connect
DescribeClusterDynamicConfiguration	授予描述集群动态配置的权限，相当于 Apache Kafka 的 DESCRIBE_CONFIGS CLUSTER ACL	List	cluster*		kafka-cluster:Connect
DescribeGroup	授予描述集群上的群组的权限，相当于 Apache Kafka 的 DESCRIBE GROUP ACL	List	group*		kafka-cluster:Connect
DescribeTopic	授予描述集群上的主题的权限，相当于 Apache Kafka 的 DESCRIBE TOPIC ACL	List	topic*		kafka-cluster:Connect

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeTopicDynamicConfiguration	授予描述集群上的主题动态配置的权限，相当于 Apache Kafka 的 DESCRIBE_CONFIGS TOPIC ACL	列表	topic*		kafka-cluster:Connect
DescribeTransactionalId	授予描述集群 IDs 上交易的权限，相当于 Apache Kafka 的 DESCRIBE TRANSACTIONAL_ID ACL	列表	transactional-id*		kafka-cluster:Connect
ReadData	授予从集群上的主题中读取数据的权限，相当于 Apache Kafka 的 READ TOPIC ACL	Read	topic*		kafka-cluster:AlterGroup kafka-cluster:Connect kafka-cluster:DescribeTopic
WriteData	授予向集群上的主题写入数据的权限，相当于 Apache Kafka 的 WRITE TOPIC ACL	Write	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopic

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
WriteDataIdempotently	授予在集群上以幂等方式写入数据的权限，相当于 Apache Kafka 的 IDEMPOTENT_WRITE CLUSTER ACL	写入	cluster*		kafka-cluster:Connect kafka-cluster:WriteData

Apache Kafka 为 APIs 亚马逊 MSK 集群定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}	

适用于 APIs 亚马逊 MSK 集群的 Apache Kafka 的条件密钥

Apache Kafka for A APIs mazon MSK 集群定义了以下条件密钥，这些条件密钥可用于 IAM `Condition` 策略的元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:ResourceTag/${TagKey}	根据附加到资源的标签键值对筛选操作。资源标签上下文密钥将仅适用于群集资源，不适用于主题、群组和交易 IDs	字符串

Amazon API Gateway 的操作、资源和条件键

Amazon API Gateway（服务前缀：`execute-api`）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon API Gateway 定义的操作
- Amazon API Gateway 定义的资源类型
- Amazon API Gateway 的条件键

Amazon API Gateway 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
InvalidateCache	用于根据客户端请求使 API 缓存失效	Write	execute-api-general*		
Invoke	用于根据客户端请求调用 API	写入	execute-api-domain		
			execute-api-general		
ManageConnections	ManageConnections 控制对 @connections API 的访问权限	写入	execute-api-general*		

Amazon API Gateway 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}	

Amazon API Gateway 的条件键

Amazon API Gateway 定义了以下条件密钥，这些条件密钥可用于 IAM 策略的Condition元素中。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
execute-api:viaDomainArn	按调用 API 的域名 ARN 筛选访问权限	字符串

Amazon App Mesh 的操作、资源和条件键

Amazon App Mesh（服务前缀:appmesh）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。

- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon App Mesh 定义的操作
- Amazon App Mesh 定义的资源类型
- Amazon App Mesh 的条件键

Amazon App Mesh 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateGatewayRoute	授予创建与虚拟网关关联的网关路由的权限	Write	gatewayRoute*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualService		
CreateMesh	授予创建服务网格的权限	Write	mesh*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateRoute	授予创建与虚拟路由器关联的路由的权限	Write	route*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualNode		
CreateVirtualGateway	授予在服务网格中创建虚拟网关的权限	Write	virtualGateway*		
				aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey}	
CreateVirtualNode	授予在服务网格中创建虚拟节点的权限	Write	virtualNode*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualService		
CreateVirtualRouter	授予在服务网格中创建虚拟路由器的权限	Write	virtualRouter*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateVirtualService	授予在服务网格中创建虚拟服务的权限	Write	virtualService*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualNode		
			virtualRouter		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteGatewayRoute	授予删除现有网关路由的权限	Write	gatewayRoute*		
DeleteMesh	授予删除现有服务网格的权限	写入	mesh*		
DeleteMeshPolicy[仅权限]	授予权限以删除网格的 RAM 访问控制策略	写入	mesh*		
DeleteRoute	授予删除现有路由的权限	Write	route*		
DeleteVirtualGateway	授予删除现有虚拟网关的权限	Write	virtualGateway*		
DeleteVirtualNode	授予删除现有虚拟节点的权限	Write	virtualNode*		
DeleteVirtualRouter	授予删除现有虚拟路由器的权限	Write	virtualRouter*		
DeleteVirtualService	授予删除现有虚拟服务的权限	Write	virtualService*		
DescribeGatewayRoute	授予描述现有网关路由的权限	Read	gatewayRoute*		
DescribeMesh	授予描述现有服务网格的权限	Read	mesh*		
DescribeRoute	授予描述现有路由的权限	Read	route*		
DescribeVirtualGateway	授予描述现有虚拟网关的权限	Read	virtualGateway*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeVirtualNode	授予描述现有虚拟节点的权限	Read	virtualNode*		
DescribeVirtualRouter	授予描述现有虚拟路由器的权限	Read	virtualRouter*		
DescribeVirtualService	授予描述现有虚拟服务的权限	读取	virtualService*		
GetMeshPolicy[仅权限]	授予权限以读取网格的 RAM 访问控制策略	读取	mesh*		
ListGatewayRoutes	授予列出服务网格中现有网关路由的权限	List	virtualGateway*		
ListMeshes	授予列出现有服务网格的权限	List			
ListRoutes	授予列出服务网格中现有路由的权限	List	virtualRouter*		
ListTagsForResource	授予列出 App Mesh 资源标签的权限	List	gatewayRoute		
			mesh		
			route		
			virtualGateway		
			virtualNode		
			virtualRouter		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			virtualService		
ListVirtualGateways	授予列出服务网格中现有虚拟网关的权限	List	mesh*		
ListVirtualNodes	授予列出现有虚拟节点的权限	List	mesh*		
ListVirtualRouters	授予列出服务网格中现有虚拟路由器的权限	List	mesh*		
ListVirtualServices	授予列出服务网格中现有虚拟服务的权限	列表	mesh*		
PutMeshPolicy[仅权限]	授予权限以定义网格的 RAM 访问控制策略	写入	mesh*		
StreamAggregatedResources	授予接收 App Mesh 端点流媒体资源的权限 (VirtualNode/VirtualGateway)	读取	virtualGateway		
			virtualNode		
TagResource	授予权限以使用指定的 resourceArn 为资源贴标签	标记	gatewayRoute		
			mesh		
			route		
			virtualGateway		
			virtualNode		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			virtualRouter		
			virtualService		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	授予权限以从资源中删除标签	标记	gatewayRoute		
			mesh		
			route		
			virtualGateway		
			virtualNode		
			virtualRouter		
			virtualService		
				aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateGatewayRoute	授予权限以更新指定服务网格和虚拟网关的现有网关路由	Write	gatewayRoute*		
			virtualService		
UpdateMesh	授予更新现有服务网格的权限	Write	mesh*		
UpdateRoute	授予更新指定服务网格和虚拟路由器的现有路由的权限	Write	route*		
			virtualNode		
UpdateVirtualGateway	授予更新指定服务网格中现有虚拟网关的权限	Write	virtualGateway*		
UpdateVirtualNode	授予更新指定服务网格中现有虚拟节点的权限	Write	virtualNode*		
UpdateVirtualRouter	授予更新指定服务网格中现有虚拟路由器的权限	Write	virtualRouter*		
UpdateVirtualService	授予更新指定服务网格中现有虚拟服务的权限	Write	virtualService*		
			virtualNode		
			virtualRouter		

Amazon App Mesh 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从

而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
mesh	arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}	aws:ResourceTag/${TagKey}
virtualService	arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualService/${VirtualServiceName}	aws:ResourceTag/${TagKey}
virtualNode	arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualNode/${VirtualNodeName}	aws:ResourceTag/${TagKey}
virtualRouter	arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${VirtualRouterName}	aws:ResourceTag/${TagKey}
route	arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${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}

Amazon App Mesh 的条件键

Amazon App Mesh 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对来筛选操作	字符串
aws:ResourceTag/${TagKey}	根据附加到资源的标签键值对来筛选操作	字符串
aws:TagKeys	根据在请求中是否具有标签键来筛选操作	ArrayOfString

Amazon AppConfig 的操作、资源和条件键

Amazon AppConfig （服务前缀:appconfig）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon AppConfig 定义的操作
- Amazon AppConfig 定义的资源类型
- Amazon AppConfig 的条件键

Amazon AppConfig 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，

以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateApplication	授予创建应用程序的权限	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfigurationProfile	授予创建配置文件的权限	Write	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateDeploymentStrategy	授予创建部署策略的权限	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironment	授予创建环境的权限	写入	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExtension	授予权限以创建扩展程序	写入		aws:RequestTag/${TagKey} aws:TagKeys	
CreateExtensionAssociation	授予权限以创建扩展程序关联	写入		aws:RequestTag/${TagKey} aws:TagKeys	
CreateHostedConfigurationVersion	授予权限以创建托管配置版本	Write	application*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			configurationprofile*		
DeleteApplication	授予删除应用程序的权限	Write	application*		
DeleteConfigurationProfile	授予删除配置文件的权限	Write	application*		
			configurationprofile*		
DeleteDeploymentStrategy	授予删除部署策略的权限	Write	deploymentstrategy*		
DeleteEnvironment	授予删除环境的权限	写入	application*		
			environment*		
DeleteExtension	授予权限以删除扩展程序	写入	extension*		
DeleteExtensionAssociation	授予权限以删除扩展程序关联	写入	extensionassociation*		
DeleteHostedConfigurationVersion	授予权限以删除托管配置版本	写入	application*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			configurationprofile*		
			hostedconfigurationversion*		
GetAccountSettings	授予查看账户 AppConfig 范围设置的权限	读取			
GetApplication	授予查看有关应用程序的详细信息的权限	Read	application*		
				aws:ResourceTag/${TagKey}	
GetConfiguration	授予查看有关配置的详细信息的权限	Read	application*		
			configurationprofile*		
			environment*		
				aws:ResourceTag/${TagKey}	
GetConfigurationProfile	授予查看有关配置文件的详细信息的权限	Read	application*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			configurationprofile*		
				aws:ResourceTag/${TagKey}	
GetDeployment	授予查看有关部署的详细信息的权限	Read	application*		
			deployment*		
			environment*		
				aws:ResourceTag/${TagKey}	
GetDeploymentStrategy	授予查看有关部署策略的详细信息的权限	Read	deploymentstrategy*		
				aws:ResourceTag/${TagKey}	
GetEnvironment	授予查看有关环境的详细信息的权限	读取	application*		
			environment*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey}	
GetExtension	授予权限以查看有关扩展程序的详细信息	读取	extension*		
				aws:ResourceTag/${TagKey}	
GetExtensionAssociation	授予权限以查看有关扩展程序关联的详细信息	读取	extensionassociation*		
				aws:ResourceTag/${TagKey}	
GetHostedConfigurationVersion	授予权限以查看有关托管配置版本的详细信息	读取	application*		
			configurationprofile*		
			hostedconfigurationversion*		
GetLatestConfiguration	授予检索部署的配置的权限	读取	configuration*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey}	
ListApplications	授予列出您账户中的应用程序的权限	List			
ListConfigurationProfiles	授予列出应用程序的配置文件的权限	List	application*		
ListDeploymentStrategies	授予列出您账户的部署策略的权限	List			
ListDeployments	授予列出环境的部署的权限	List	application*		
			environment*		
ListEnvironments	授予列出应用程序的环境的权限	列表	application*		
ListExtensionAssociations	授予权限以列出您账户中的扩展程序关联	列表			
ListExtensions	授予权限以列出您账户中的扩展程序	列表			
ListHostedConfigurationVersions	授予权限以列出配置文件的托管配置版本	List	application*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			configurationprofile*		
ListTagsForResource	授予权限以查看指定资源的资源标签的列表	读取	application		
			configurationprofile		
			deployment		
			deploymentstrategy		
			environment		
			extension		
			extensionassociation		
				aws:ResourceTag/${TagKey}	
StartConfigurationSession	授予启动配置会话的权限	写入	configuration*		
				aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StartDeployment	授予启动部署的权限	Write	application*		
			configurationprofile*		
			deploymentstrategy*		
			environment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StopDeployment	授予停止部署的权限	写入	application*		
			deployment*		
			environment*		
TagResource	授予标记应用配置资源的权限	标记	application		
			configuration		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			configurationprofile		
			deployment		
			deploymentstrategy		
			environment		
			extension		
			extensionassociation		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	授予取消标记应用配置资源的权限	标记	application		
			configuration		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			configurationprofile		
			deployment		
			deploymentstrategy		
			environment		
			extension		
			extensionassociation		
				aws:TagKeys	
UpdateAccountSettings	授予修改账户 AppConfig 范围设置的权限	写入			
UpdateApplication	授予修改应用程序的权限	Write	application*		
				aws:ResourceTag/${TagKey}	
UpdateConfigurationProfile	授予修改配置文件的权限	Write	application*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			configurationprofile*		
				aws:ResourceTag/${TagKey}	
UpdateDeploymentStrategy	授予修改部署策略的权限	Write	deploymentstrategy*		
				aws:ResourceTag/${TagKey}	
UpdateEnvironment	授予修改环境的权限	写入	application*		
			environment*		
				aws:ResourceTag/${TagKey}	
UpdateExtension	授予权限以修改扩展程序	写入	extension*		
				aws:ResourceTag/${TagKey}	
UpdateExtensionAssociation	授予权限以修改扩展程序关联	写入	extensionassociation*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey}	
ValidateConfiguration	授予验证配置的权限	写入	application*		
			configurationprofile*		

Amazon AppConfig 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
application	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}	aws:ResourceTag/${TagKey}
environment	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/environment/${EnvironmentId}	aws:ResourceTag/${TagKey}
configurationprofile	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/configurationprofile/${ConfigurationProfileId}	aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
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/${TagKey}
extensionassociation	arn:${Partition}:appconfig:${Region}:${Account}:extensionassociation/${ExtensionAssociationId}	aws:ResourceTag/${TagKey}

Amazon AppConfig 的条件键

Amazon AppConfig 定义了可在 IAM 策略Condition元素中使用的以下条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据指定标签的允许值集筛选访问权限	字符串
aws:ResourceTag/${TagKey}	通过分配给资源的标签键值对筛选访问权限 Amazon	字符串
aws:TagKeys	按请求中允许的标签键列表筛选访问	ArrayOfString

Amazon Application Auto Scaling 的操作、资源和条件键

Amazon Application Auto Scaling（服务前缀:application-autoscaling）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Application Auto Scaling 定义的操作
- Amazon Application Auto Scaling 定义的资源类型
- Amazon Application Auto Scaling 的条件键

Amazon Application Auto Scaling 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须

具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteScalingPolicy	授予权限以删除扩缩策略	写入	ScalableTarget*		
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteScheduledAction	授予删除计划操作的权限	写入	ScalableTarget*		
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
DeregisterScalableTarget	授予取消注册可扩展目标的权限	写入	ScalableTarget*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
DescribeScalableTargets	授予权限以描述指定命名空间中的一个或多个可扩展目标	读取			
DescribeScalingActivities	授予权限以描述指定命名空间中的一组扩缩活动或所有扩缩活动	读取			
DescribeScalingPolicies	授予权限以描述指定命名空间中的一组扩缩策略或所有扩缩策略	读取			
DescribeScheduledActions	授予权限以描述指定命名空间中的一组计划操作或所有计划操作	读取			
GetPredictiveScalingForecast	授予权限以检索预测性扩展策略的预测数据	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListTagsForResource	授予权限以列出可扩展目标的标签	读取	ScalableTarget*		
PutScalingPolicy	授予权限以为可扩展目标创建和更新扩缩策略	写入	ScalableTarget*		
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
PutScheduledAction	授予权限以为可扩展目标创建和更新计划操作	写入	ScalableTarget*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
RegisterScalableTarget	授予在 Application Auto Scaling 中注册 Amazon 或自定义资源作为可扩展目标以及更新用于管理可扩展目标的配置参数的权限	写入	ScalableTarget*		application-autoscaling:TagResource

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
TagResource	授予权限以标记可扩展目标	标记	ScalableTarget*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予权限以从可扩展目标中删除标记	标记	ScalableTarget*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys	

Amazon Application Auto Scaling 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
ScalableTarget	arn:${Partition}:application-autoscaling:${Region}:${Account}:scalable-target/${ResourceId}	aws:ResourceTag/${TagKey}

Amazon Application Auto Scaling 的条件键

Amazon Application Auto Scaling 定义了以下可以在 IAM 策略Condition元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
application-autoscaling:scalable-dimension	按请求中传递的可扩展维度筛选访问	字符串
application-autoscaling:service-namespace	按请求中传递的服务命名空间筛选访问	字符串

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString

Amazon 应用程序恢复控制器的操作、资源和条件键-Zonal Shift

Amazon Application Recovery Controller-Zonal Shift（服务前缀:`arc-zonal-shift`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- 由 Amazon 应用程序恢复控制器定义的操作-区域移动
- 由 Amazon 应用程序恢复控制器定义的资源类型-区域移动
- Amazon 应用程序恢复控制器的条件密钥-区域移动

由 Amazon 应用程序恢复控制器定义的操作-区域移动

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须

具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CancelZonalShift	授予权限以取消活动区域移动	写入	ALB*		
			NLB*		
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreatePracticeRunConfiguration	授予创建练习运行配置的权限	写入	ALB*		cloudwatch:DescribeAlarms iam:CreateServiceLinkedRole
			NLB*		
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeletePracticeRunConfiguration	授予删除练习运行配置的权限	写入	ALB*		
			NLB*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
GetAutoshiftObserverNotificationStatus	授予权限以获取自动转移观察器通知状态	读取			
GetManagedResource	授予权限以获取有关托管资源的信息	读取	ALB*		
			NLB*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ListAutoshifts	授予列出活动和已完成自动转移的权限	列表			
ListManagedResources	授予权限以列出托管资源	列表			
ListZonalShifts	授予权限以列出区域移动	列表			
StartZonalShift	授予权限以开始区域移动	写入	ALB*		
			NLB*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
UpdateAutoshiftObserverNotificationStatus	授予权限以更新自动转移观察器通知状态	写入			
UpdatePracticeRunConfiguration	授予更新练习运行配置的权限	写入	ALB*		cloudwatch:DescribeAlarms iam:CreateServiceLinkedRole
			NLB*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
UpdateZonalAutoshiftConfiguration	授予更新可用区自动转移状态的权限	写入	ALB*		
			NLB*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
UpdateZonalShift	授予权限以更新现有区域移动	写入	ALB*		
			NLB*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

由 Amazon 应用程序恢复控制器定义的资源类型-区域移动

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
ALB	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/app/${LoadBalancerName}/${LoadBalancerId}	arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
		elasticloadbalancing:ResourceTag/${TagKey}
NLB	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/net/${LoadBalancerName}/${LoadBalancerId}	arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

Amazon 应用程序恢复控制器的条件密钥-区域移动

Amazon 应用程序恢复控制器-区域转移定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
arc-zonal-shift:ResourceIdentifier	按托管资源的资源标识符筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与托管资源关联的标签筛选访问	字符串
elasticloadbalancing:ResourceTag/${TagKey}	按与托管资源关联的标签筛选访问	字符串

Amazon AppSync 的操作、资源和条件键

Amazon AppSync （服务前缀:appsync）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon AppSync 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateApi	授予将 GraphQL API 附加到中的自定义域名的权限 AppSync	写入	domain*		
AssociateMergedGraphqlApi	授予将合并的 API 与源 API 关联的权限	写入	graphqlapi*		
AssociateSourceGraphqlApi	授予将源 API 与合并的 API 关联的权限	写入	graphqlapi*		
CreateApi	授予创建 API 的权限	写入		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole
CreateApiCache	授予在中创建 API 缓存的权限 AppSync	写入			
CreateApiKey	授予创建唯一密钥以分发到执行您的 API 的客户端的权限	写入			
CreateChannelNamespace	授予创建频道命名空间的权限	写入	channelNamespace*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSource	授予创建数据源的权限	写入			
CreateDomainName	授予在中创建自定义域名的权限 AppSync	写入		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateFunction	授予创建新函数的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateGraphqlApi	授予创建 GraphQL API 的权限，这是顶级资源 AppSync	写入		aws:RequestTag/${TagKey} aws:TagKeys appsync:Visibility	iam:CreateServiceLinkedRole
CreateResolver	授予权限以创建解析程序。解析程序可将传入请求转换为数据源可以理解的格式，并将数据源的响应转换为 GraphQL	写入			
CreateType	授予权限以创建类型。	写入			
DeleteApi	授予删除 API 的权限。这还将清理该 API 下的所有 AppSync 资源	写入	api*		
				aws:ResourceTag/${TagKey}	
DeleteApiCache	授予在中删除 API 缓存的权限 AppSync	写入			
DeleteApiKey	授予删除 API 密钥的权限	写入			
DeleteChannelNamespace	授予删除频道命名空间的权限	写入	channelNamespace*		
				aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteDataSource	授予删除数据源的权限	写入			
DeleteDomainName	授予删除自定义域名的权限 AppSync	写入	domain*		
				aws:ResourceTag/${TagKey}	
DeleteFunction	授予权限以删除函数	写入			
DeleteGraphqlApi	授予权限以删除 GraphQL API。这还将清理该 API 下的所有 AppSync 资源	写入	graphqlapi*		
				aws:ResourceTag/${TagKey}	
DeleteResolver	授予权限以删除解析程序	写入			
DeleteResourcePolicy[仅权限]	授予删除资源策略的权限	写入			
DeleteType	授予删除类型的权限。	写入			
DisassociateApi	授予将 GraphQL API 与中的自定义域名分离 AppSync	写入	domain*		
DisassociateMergedGraphqlApi	授予从源 API 识别的合并 API 中删除关联的源 API 的权限	写入	mergedApiAssociation*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DisassociateSourceGraphqlApi	授予从合并的 API 识别的合并 API 中删除关联的源 API 的权限	写入	sourceApiAssociation*		
EvaluateCode	授予使用运行时和上下文评估代码的权限	读取			
EvaluateMappingTemplate	授予权限以评估模板映射	读取			
EventConnect	授予连接活动 API 的权限	写入	api*		
EventPublish	授予将事件发布到频道命名空间的权限	写入	channelNamespace*		
EventSubscribe	授予订阅频道命名空间的权限	写入	channelNamespace*		
FlushApiCache	授予刷新 API 缓存的权限 AppSync	写入			
GetApi	授予检索 API 的权限	读取	api*		
				aws:ResourceTag/${TagKey}	
GetApiAssociation	授予读取自定义域名的权限-GraphQL API 关联详情 AppSync	读取	domain*		
GetApiCache	授予读取有关 API 缓存信息的权限 AppSync	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetChannelNamespace	授予检索频道命名空间的权限	读取	channelNamespace*		
				aws:ResourceTag/${TagKey}	
GetDataSource	授予检索数据来源的权限	读取			
GetDataSourceIntrospection	授予检索数据来源自检的权限	读取			
GetDomainName	授予读取有关自定义域名的信息的权限 AppSync	读取	domain*		
				aws:ResourceTag/${TagKey}	
GetFunction	授予检索函数的权限	读取			
GetGraphqlApi	授予检索 GraphQL API 的权限	读取	graphqlapi*		
				aws:ResourceTag/${TagKey}	
GetGraphqlApiEnvironmentVariables	授予权限以检索 GraphQL API 的环境变量	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetIntrospectionSchema	授予检索 GraphQL API 的自检架构的权限	读取			
GetResolver	授予检索解析程序的权限	读取			
GetResourcePolicy[仅权限]	授予读取资源策略的权限	读取			
GetSchemaCreationStatus	授予检索架构创建操作当前状态的权限	读取			
GetSourceApiAssociation	授予读取有关合并 API 关联的源 API 的信息的权限	读取	sourceApiAssociation*		
GetType	授予权限以检索类型	读取			
GraphQL[仅权限]	授予向 GraphQL API 发送 GraphQL 查询的权限	写入	field*		
			graphqlapi*		
ListApiKeys	授予列出给定 API 的 API 密钥的权限	列表			
ListApis	授予上架权限 APIs	列表		aws:ResourceTag/${TagKey}	
ListChannelNamespaces	授予列出频道命名空间的权限	列表	api*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey}	
ListDataSources	授予列出给定 API 的数据源的权限	列表			
ListDomainNames	授予枚举自定义域名的权限 AppSync	列表		aws:ResourceTag/${TagKey}	
ListFunctions	授予列出给定 API 的函数的权限	列表			
ListGraphqlApis	授予列出 GraphQL 的权限 APIs	列表			
ListResolvers	授予列出给定 API 和类型的解析程序的权限	列表			
ListResolversByFunction	授予列出与特定函数关联的解析程序的权限	列表			
ListSourceApiAssociations	授予列出与给定合并 API APIs 关联的源的权限	列表			
ListTagsForResource	授予列出资源标签的权限	读取	api		
			channelNamespace		
			domain		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			graphqlapi		
				aws:ResourceTag/${TagKey}	
ListTypes	授予列出给定 API 类型的权限	列表			
ListTypesByAssociation	授予列出给定的合并 API 和源 API 关联的类型的权限	列表			
PutGraphqlApiEnvironmentVariables	授予权限以更新 GraphQL API 的环境变量	写入			
PutResourcePolicy[仅权限]	授予设置资源策略的权限	写入			
SetWebACL	授予设置 Web ACL 的权限	写入			
SourceGraphQL[仅权限]	授予将 GraphQL 查询发送到合并 API 的源 API 的权限	写入	field*		
			graphqlapi*		
StartDataSourceIntrospection	授予进行数据来源自检的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StartSchemaCreation	授予向 GraphQL API 添加新架构的权限。此操作是异步的-GetSchemaCreationStatus 可以显示何时完成	写入			
StartSchemaMerge	授予为给定的合并 API 和关联的源 API 启动架构合并的权限	写入	sourceApiAssociation*		
TagResource	授予权限以标记资源	Tagging	api		
			channelNamespace		
			domain		
			graphqlapi		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	授予权限以取消标记资源	标记	api		
			channelNamespace		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			domain		
			graphqlapi		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateApi	授予更新 API 的权限	写入	api*		iam:CreateServiceLinkedRole
				aws:ResourceTag/${TagKey}	
UpdateApiCache	授予更新 API 缓存的权限 AppSync	写入			
UpdateApiKey	授予更新给定 API 的 API 密钥的权限	写入			
UpdateChannelNamespace	授予更新频道命名空间的权限	写入	channelNamespace*		
				aws:ResourceTag/${TagKey}	
UpdateDataSource	授予权限以更新数据源	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateDomainName	授予更新自定义域名的权限 AppSync	写入	domain*		
				aws:ResourceTag/${TagKey}	
UpdateFunction	授予更新现有函数对象的权限	写入			
UpdateGraphqlApi	授予权限以更新 GraphQL API	写入	graphqlapi*		iam:CreateServiceLinkedRole
				aws:ResourceTag/${TagKey}	
UpdateResolver	授予权限以更新预留程序	写入			
UpdateSourceApiAssociation	授予更新合并的 API 源 API 关联的权限	写入	sourceApiAssociation*		
UpdateType	授予权限以更新类型	写入			

Amazon AppSync 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}

资源类型	ARN	条件键
channelNamespace	arn:${Partition}:appsync:${Region}:${Account}:apis/${ApiId}/channelNamespace/${ChannelNamespaceName}	aws:ResourceTag/${TagKey}

Amazon AppSync 的条件键

Amazon AppSync 定义了可在 IAM 策略Condition元素中使用的以下条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
appsync:Visibility	按 API 的可见性筛选访问权限	字符串
aws:RequestTag/${TagKey}	按请求中的标签键值对筛选访问	字符串
aws:ResourceTag/${TagKey}	按附加到资源的标签键值对筛选访问权限	字符串
aws:TagKeys	根据在请求中是否具有标签键来筛选访问	ArrayOfString

Amazon Athena 的操作、资源和条件键

Amazon Athena（服务前缀：athena）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon Athena 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchGetNamedQuery	授予获取一个或多个命名查询相关信息的权限	读取	workgroup *		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchGetPreparedStatement	授予权限以获取有关一或多个准备语句的信息	读取	workgroup*		
BatchGetQueryExecution	授予获取一个或多个查询执行相关信息的权限	读取	workgroup*		
CancelCapacityReservation	授予权限以取消容量预留	写入	capacity-reservation*		
CancelQueryExecution	授予取消查询执行的权限。已淘汰。仅适用于使用 1.1.0 之前版本的 Athena JDBC 驱动程序的 Amazon 服务和主体。StopQueryExecution 否则使用	写入	workgroup*		
CreateCapacityReservation	授予权限以创建容量预留	写入	capacity-reservation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataCatalog	授予创建数据目录的权限	写入	datacatalog*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNamedQuery	授予创建命名查询的权限	写入	workgroup*		
CreateNotebook	授予权限以创建笔记本	写入	workgroup*		
CreatePreparedStatement	授予创建准备语句的权限。	写入	workgroup*		
CreatePresignedNotebookUrl	授予权限以创建预签名笔记本 URL	写入	workgroup*		
CreateWorkGroup	授予创建工作组的权限	写入	workgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCapacityReservation	授予权限以删除容量预留	写入	capacity-reservation*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteDataCatalog	授予删除数据目录的权限	写入	datacatalog*		
DeleteNamedQuery	授予删除指定命名查询的权限	写入	workgroup*		
DeleteNotebook	授予权限以删除笔记本	写入	workgroup*		
DeletePreparedStatement	授予删除指定的准备语句的权限。	写入	workgroup*		
DeleteWorkGroup	授予删除工作组的权限	写入	workgroup*		
ExportNotebook	授予权限以导出笔记本	写入	workgroup*		
GetCalculationExecution	授予权限以获取计算执行	读取	workgroup*		
GetCalculationExecutionCode	授予权限以获取计算执行代码	读取	workgroup*		
GetCalculationExecutionStatus	授予权限以获取计算执行状态	读取	workgroup*		
GetCapacityAssignmentConfiguration	授予获取容量预留的容量分配信息的权限	读取	capacity-reservation*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetCapacityReservation	授予权限以获取容量预留	读取	capacity-reservation*		
GetCatalogs	授予启用对数据库和表的访问的权限。仅适用于使用 Athena JDBC 驱动程序 1.1.0 版的 Amazon 服务托管策略和主体	读取			
GetDataCatalog	授予获取数据目录的权限	读取	datacatalog*		
GetDatabase	授予获取给定数据目录的数据库的权限	读取	datacatalog*		
GetExecutionEngine	授予启用对指定数据库和表的访问的权限。仅适用于使用 Athena JDBC 驱动程序 1.1.0 版的 Amazon 服务托管策略和主体	读取			
GetExecutionEngines	授予启用对数据库和表的访问的权限。仅适用于使用 Athena JDBC 驱动程序 1.1.0 版的 Amazon 服务托管策略和主体	读取			
GetNamedQuery	授予获取指定命名查询相关信息的权限	读取	workgroup*		
GetNamespace	授予启用对指定数据库和表的访问的权限。仅适用于使用 Athena JDBC 驱动程序 1.1.0 版的 Amazon 服务托管策略和主体	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetNamespaces	授予启用对数据库和表的访问的权限。仅适用于使用 Athena JDBC 驱动程序 1.1.0 版的 Amazon 服务托管策略和主体	读取			
GetNotebookMetadata	授予权限以获取笔记本元数据	读取	workgroup *		
GetPreparedStatement	授予获取指定准备语句相关信息的权限。	读取	workgroup *		
GetQueryExecution	授予获取指定查询执行相关信息的权限	读取	workgroup *		
GetQueryExecutions	授予获取查询执行的权限。已淘汰。仅适用于使用 1.1.0 之前版本的 Athena JDBC 驱动程序的 Amazon 服务和主体。ListQueryExecutions 否则使用	读取			
GetQueryResults	授予获取查询结果的权限	读取	workgroup *		
GetQueryResultsStream	授予获取查询结果流的权限	读取	workgroup *		
GetQueryRuntimeStatistics	授予权限以获取指定查询执行的运行时统计数据	读取	workgroup *		
GetSession	授予权限以获取会话	读取	workgroup *		
GetSessionStatus	授予权限以获取会话状态	读取	workgroup *		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetTable	授予启用对指定表的访问的权限。仅适用于使用 Athena JDBC 驱动程序 1.1.0 版的 Amazon 服务托管策略和主体	读取			
GetTableMetadata	授予获取有关给定数据目录的表的元数据的权限	读取	datacatalog*		
GetTables	授予启用对表的访问的权限。仅适用于使用 Athena JDBC 驱动程序 1.1.0 版的 Amazon 服务托管策略和主体	读取			
GetWorkGroup	授予获取工作组的权限	读取	workgroup*		
ImportNotebook	授予权限以导入笔记本	写入	workgroup*		
ListApplicationDPUSizes	授予返回列表的权限 ApplicationRuntimeIds	列表			
ListCalculationExecutions	授予权限以返回计算执行的列表	列表	workgroup*		
ListCapacityReservations	授予返回指定容量预留列表的权限 Amazon Web Services 账户	列表			
ListDataCatalogs	授予返回指定数据目录列表的权限 Amazon Web Services 账户	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListDatabases	授予返回给定数据目录的数据库列表的权限	列表	datacatalog*		
ListEngineVersions	授予返回指定的 athena 引擎版本列表的权限 Amazon Web Services 账户	读取			
ListExecutors	授予权限以返回执行程序的列表	列表			
ListNamedQueries	授予在 Amazon Athena 中返回指定查询列表的权限 Amazon Web Services 账户	列表	workgroup*		
ListNotebookMetadata	授予权限以返回给定工作组的笔记本列表	列表	workgroup*		
ListNotebookSessions	授予权限以返回给定笔记本的会话列表	列表	workgroup*		
ListPreparedStatements	授予返回指定工作组的准备语句列表的权限。	列表	workgroup*		
ListQueryExecutions	授予返回指定查询执行列表的权限 Amazon Web Services 账户	读取	workgroup*		
ListSessions	授予权限以返回给定工作组的会话列表	列表	workgroup*		
ListTableMetadata	授予返回给定数据目录的数据库中表元数据列表的权限	读取	datacatalog*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListTagsForResource	授予返回资源标签列表的权限	读取	capacity-reservation*		
			datacatalog*		
			workgroup*		
ListWorkGroups	授予返回指定工作组列表的权限 Amazon Web Services 账户	列表			
PutCapacityAssignmentConfiguration	授予将容量预留中的容量分配给查询的权限	写入	capacity-reservation*		
			workgroup*		
RunQuery	授予运行查询的权限。已淘汰。仅适用于使用 1.1.0 之前版本的 Athena JDBC 驱动程序的 Amazon 服务和主体。StartQueryExecution 否则使用	写入			
StartCalculationExecution	授予权限以开始计算执行	写入	workgroup*		
StartQueryExecution	授予使用作为字符串提供的 SQL 查询启动查询执行的权限	写入	workgroup*		
StartSession	授予权限以开启会话	写入	workgroup*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StopCalculationExecution	授予权限以停止计算执行	写入	workgroup*		
StopQueryExecution	授予停止指定查询执行的权限	写入	workgroup*		
TagResource	授予权限以将标签添加到资源	标记	capacity-reservation*		
			datacatalog*		
			workgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TerminateSession	授予权限以终止会话	写入	workgroup*		
UntagResource	授予权限以从资源中删除标签	标记	capacity-reservation*		
			datacatalog*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			workgroup*		
				aws:TagKeys	
UpdateCapacityReservation	授予权限以更新容量预留	写入	capacity-reservation*		
UpdateDataCatalog	授予更新数据目录的权限	写入	datacatalog*		
UpdateNamedQuery	授予更新指定命名查询的权限	写入	workgroup*		
UpdateNotebook	授予权限以更新笔记本	写入	workgroup*		
UpdateNotebookMetadata	授予权限以更新笔记本元数据	写入	workgroup*		
UpdatePreparedStatement	授予更新准备语句的权限。	写入	workgroup*		
UpdateWorkGroup	授予更新工作组的权限	写入	workgroup*		

Amazon Athena 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从

而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
datacatalog	`arn:${Partition}:athena:${Region}:${Account}:datacatalog/${DataCatalogName}`	aws:ResourceTag/${TagKey}
workgroup	`arn:${Partition}:athena:${Region}:${Account}:workgroup/${WorkGroupName}`	aws:ResourceTag/${TagKey}
capacity-reservation	`arn:${Partition}:athena:${Region}:${Account}:capacity-reservation/${CapacityReservationName}`	aws:ResourceTag/${TagKey}

Amazon Athena 的条件键

Amazon Athena 定义以下可以在 IAM policy 的 `Condition` 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对来筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按附加到资源的标签键值对筛选访问权限	字符串
aws:TagKeys	根据在请求中是否具有标签键来筛选访问	ArrayOfString

Amazon Backup 的操作、资源和条件键

Amazon Backup（服务前缀:backup）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon Backup 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CancelLegalHold	授予权限以取消合法保留	写入	legalHold*		
CopyFromBackupVault[仅权限]	授予权限以从备份文件库复制	Write	recoveryPoint*		
				backup:CopyTargets backup:CopyTargetOrgPaths	
CopyIntoBackupVault[仅权限]	授予权限以复制到备份文件库	Write	backupVault*		
				aws:RequestTag/${TagKey}	
CreateBackupPlan	授予权限以创建新的备份计划	Write	backupPlan*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBackupSelection	授予权限以在备份计划中创建新的资源分配	Write	backupPlan*		iam:PassRole

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateBackupVault	授予权限以创建新的备份文件库	写入	backupVault*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFramework	授予权限以新建框架	写入	framework*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLegalHold	授予权限以创建新的合法保留	写入	legalHold*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLogicallyAirGappedBackupVault	授予创建新的逻辑间隙备份库（存储备份的逻辑容器）的权限	写入	backupVault*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys backup:MinRetentionDays backup:MaxRetentionDays	
CreateReportPlan	授予权限以创建新的报告计划	写入	reportPlan*		
				aws:RequestTag/${TagKey} aws:TagKeys backup:FrameworkArns	
CreateRestoreTestingPlan	授予创建新还原测试计划的权限	写入	restoreTestingPlan*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRestoreTestingSelection	授予在还原测试计划中创建新资源分配的权限	写入	restoreTestingPlan*		iam:PassRole
DeleteBackupPlan	授予权限以删除备份计划	Write	backupPlan*		
DeleteBackupSelection	授予权限以从备份计划中删除资源分配	Write	backupPlan*		
DeleteBackupVault	授予权限以删除备份文件库	Write	backupVault*		
DeleteBackupVaultAccessPolicy	授予权限以删除备份文件库访问策略	权限管理	backupVault*		
DeleteBackupVaultLockConfiguration	授予权限以从备份文件库中删除锁定配置	写入	backupVault*		
DeleteBackupVaultNotifications	授予权限以从备份文件库中删除通知	写入	backupVault*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteBackupVaultSharingPolicy[仅权限]	授予权限以删除备份文件库共享策略	权限管理	backupVault*		
DeleteFramework	授予权限以删除框架	写入	framework*		
DeleteRecoveryPoint	授予权限以从备份文件库中删除恢复点	写入	recoveryPoint*		
DeleteReportPlan	授予权限以删除报告计划	写入	reportPlan*		
DeleteRestoreTestingPlan	授予删除还原测试计划的权限	写入	restoreTestingPlan*		
DeleteRestoreTestingSelection	授予从还原测试计划中删除资源分配的权限	写入	restoreTestingPlan*		
DescribeBackupJob	授予权限以描述备份作业	Read			
DescribeBackupVault	授予权限以使用指定名称描述新的备份文件库	Read	backupVault*		
DescribeCopyJob	授予权限以描述复制作业	读取			
DescribeFramework	授予权限以描述具有指定名称的框架	读取	framework*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeGlobalSettings	授予权限以描述全局设置	Read			
DescribeProtectedResource	授予权限以描述受保护资源	Read			
DescribeRecoveryPoint	授予权限以描述恢复点	Read	recoveryPoint*		
DescribeRegionSettings	授予权限以描述区域设置	读取			
DescribeReportJob	授予权限以描述报告作业	读取			
DescribeReportPlan	授予权限以描述具有指定名称的报告计划	读取	reportPlan*		
DescribeRestoreJob	授予权限以描述还原作业	Read			
DisassociateRecoveryPoint	授予权限以从备份文件库中取消恢复点的关联	写入	recoveryPoint*		
DisassociateRecoveryPointFromParent	授予权限以从父项中取消恢复点的关联	写入	recoveryPoint*		
ExportBackupPlanTemplate	授予权限以将备份计划导出为 JSON	Read			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetBackupPlan	授予权限以获取备份计划	Read	backupPlan*		
GetBackupPlanFromJSON	授予权限以将 JSON 转换为备份计划	Read			
GetBackupPlanFromTemplate	授予权限以将模板转换为备份计划	Read			
GetBackupSelection	授予权限以获取备份计划资源分配	Read	backupPlan*		
GetBackupVaultAccessPolicy	授予权限以获取备份文件库访问策略	Read	backupVault*		
GetBackupVaultNotifications	授予权限以获取备份文件库通知	读取	backupVault*		
GetBackupVaultSharingPolicy[仅权限]	授予权限以获取备份文件库共享策略	读取	backupVault*		
GetLegalHold	授予权限以获取合法保留	读取	legalHold*		
GetRecoveryPointIndexDetails	授予获取恢复点索引详细信息的权限	读取	recoveryPoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetRecoveryPointRestoreMetadata	授予权限以获取恢复点还原元数据	读取	recoveryPoint*		
GetRestoreJobMetadata	授予获取还原作业所关联还原元数据的权限	读取			
GetRestoreTestingInferredMetadata	授予获取还原测试所生成的推断元数据的权限	读取			
GetRestoreTestingPlan	授予获取还原测试计划的权限	读取	restoreTestingPlan*		
GetRestoreTestingSelection	授予获取还原测试计划资源分配的权限	读取	restoreTestingPlan*		
GetSupportedResourceTypes	授予权限以获取支持的资源类型	读取			
ListBackupJobSummaries	授予列出备份作业摘要的权限	列表			
ListBackupJobs	授予权限以列出备份作业	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListBackupPlanTemplates	授予列出 Backup 提供的 Amazon 备份计划模板的权限	列表			
ListBackupPlanVersions	授予权限以列出备份计划版本	列表	backupPlan*		
ListBackupPlans	授予权限以列出备份计划	列表			
ListBackupSelections	授予权限以列出特定备份计划的资源分配	列表	backupPlan*		
ListBackupVaults	授予权限以列出备份文件库	列表			
ListCopyJobSummaries	授予列出复制作业摘要的权限	列表			
ListCopyJobs	授予权限以列出复制作业	列表			
ListFrameworks	授予权限以列出框架	列表			
ListIndexedRecoveryPoints	授予获取列表索引恢复点的权限	列表			
ListIndexedRecoveryPointsForSearch[仅权限]	授予列出已编入索引的恢复点以进行搜索的权限	权限管理			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListLegalHolds	授予权限以列出合法保留	列表			
ListProtectedResources	授予通过 B Amazon ackup 列出受保护资源的权限	列表			
ListProtectedResourcesByBackupVault	授予权限以列出备份文件库内受保护的资源	列表	backupVault*		
ListRecoveryPointsByBackupVault	授予权限以列出备份文件库中的恢复点	列表	backupVault*		
ListRecoveryPointsByLegalHold	授予权限以按合法保留列出恢复点	列表	legalHold*		
ListRecoveryPointsByResource	授予权限以列出资源恢复点	列表			
ListReportJobs	授予列出报告作业的权限。	列表			
ListReportPlans	授予列出报告计划的权限。	列表			
ListRestoreJobSummaries	授予列出还原作业摘要的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListRestoreJobs	授予列出还原作业的权限	列表			
ListRestoreJobsByProtectedResource	授予列出受保护资源的还原作业的权限	列表			
ListRestoreTestingPlans	授予列出还原测试计划的权限	列表			
ListRestoreTestingSelections	授予列出特定还原测试计划的资源分配的权限	列表	restoreTestingPlan *		
ListTags	授予权限以列出资源的标签	Read	backupPlan		
			backupVault		
			framework		
			legalHold		
			recoveryPoint		
			reportPlan		
			restoreTestingPlan		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutBackupVaultAccessPolicy	授予权限以将访问策略添加到备份文件库中	权限管理	backupVault*		
PutBackupVaultLockConfiguration	授予权限以向备份文件库添加锁定配置	写入	backupVault*		
				backup:ChangeableForDays backup:MinRetentionDays backup:MaxRetentionDays	
PutBackupVaultNotifications	授予权限以将 SNS 主题添加到备份文件库中	写入	backupVault*		
PutBackupVaultSharingPolicy[仅权限]	授予权限以将共享策略添加到备份文件库中	权限管理	backupVault*		
PutRestoreValidationResult	授予放置还原验证结果的权限	写入			
SearchRecoveryPoint[仅权限]	授予搜索恢复点的权限	权限管理	recoveryPoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StartBackupJob	授予权限以启动新的备份作业	Write	backupVault*		iam:PassRole
StartCopyJob	授予权限以将备份从源备份文件库复制到目标备份文件库	写入	recoveryPoint*		iam:PassRole
StartReportJob	授予权限以启动新的报告作业	写入	reportPlan*		
StartRestoreJob	授予权限以启动新的还原作业	Write	recoveryPoint*		iam:PassRole
StopBackupJob	授予权限以停止备份作业	Write			
TagResource	授予权限以标记资源	Tagging	backupPlan		
			backupVault		
			framework		
			legalHold		
			recoveryPoint		
			reportPlan		
			restoreTestingPlan		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予权限以取消标记资源	Tagging	backupPlan		
			backupVault		
			framework		
			legalHold		
			recoveryPoint		
			reportPlan		
			restoreTestingPlan		
				aws:TagKeys	
UpdateBackupPlan	授予权限以更新备份计划	写入	backupPlan*		
UpdateFramework	授予更新框架的权限	写入	framework*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateGlobalSettings	授予更新 Amazon 账户当前全局设置的权限	写入			
UpdateRecoveryPointIndexSettings	授予更新恢复点索引设置的权限	写入	recoveryPoint*		
				backup:Index	
UpdateRecoveryPointLifecycle	授予权限以更新恢复点生命周期	Write	recoveryPoint*		
UpdateRegionSettings	授予权限以更新区域当前选择加入服务设置	写入			
UpdateReportPlan	授予权限以更新报告计划	写入	reportPlan*		
				backup:FrameworkArns	
UpdateRestoreTestingPlan	授予更新还原测试计划的权限	写入	restoreTestingPlan*		
UpdateRestoreTestingSelection	授予更新还原测试计划中的资源分配的权限	写入	restoreTestingPlan*		iam:PassRole

Amazon Backup 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}

Amazon Backup 的条件键

Amazon Backup 定义了以下可在 IAM 策略Condition元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按每个标签的允许值集筛选访问	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中是否具有必需标签来筛选访问	ArrayOfString
backup:ChangeableForDays	按 ChangeableForDays 参数值筛选访问权限	数值
backup:CopyTargetOrgPaths	按组织单位筛选访问	ArrayOfString
backup:CopyTargets	按备份文件库的 ARN 筛选访问	ArrayOfARN
backup:FrameworkArns	筛选框架访问权限 ARNs	ArrayOfARN
backup:Index	按索引参数的值筛选访问权限	字符串
backup:MaxRetentionDays	按 MaxRetentionDays 参数值筛选访问权限	数值
backup:MinRetentionDays	按 MinRetentionDays 参数值筛选访问权限	数值

Amazon Backup Gateway 的操作、资源和条件键

Amazon Backup Gateway（服务前缀:backup-gateway）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon Backup Gateway 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateGatewayToServer	授予权限 AssociateGatewayToServer	写入	gateway*		
			hypervisor*		
Backup	授予 Backup 的权限	写入	virtualmachine*		
CreateGateway	授予权限 CreateGateway	写入		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteGateway	授予权限 DeleteGateway	写入	gateway*		
DeleteHypervisor	授予权限 DeleteHypervisor	写入	hypervisor*		
DisassociateGatewayFromServer	授予权限 DisassociateGatewayFromServer	写入	gateway*		
GetBandwidthRateLimitSchedule	授予权限 GetBandwidthRateLimitSchedule	读取	gateway*		
GetGateway	授予权限 GetGateway	读取	gateway*		
GetHypervisor	授予权限 GetHypervisor	读取	hypervisor*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetHypervisorPropertyMappings	授予权限 GetHypervisorPropertyMappings	读取	hypervisor*		
GetVirtualMachine	授予权限 GetVirtualMachine	读取	virtualmachine*		
ImportHypervisorConfiguration	授予权限 ImportHypervisorConfiguration	写入		aws:RequestTag/${TagKey} aws:TagKeys	
ListGateways	授予权限 ListGateways	读取			
ListHypervisors	授予权限 ListHypervisors	读取			
ListTagsForResource	授予权限 ListTagsForResource	读取	gateway		
			hypervisor		
			virtualmachine		
ListVirtualMachines	授予权限 ListVirtualMachines	读取			
PutBandwidthRateLimitSchedule	授予权限 PutBandwidthRateLimitSchedule	写入	gateway*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutHypervisorPropertyMappings	授予权限 PutHypervisorPropertyMappings	写入	hypervisor*		iam:PassRole
PutMaintenanceStartTime	授予权限 PutMaintenanceStartTime	写入	gateway*		
Restore	授予 Restore 的权限	写入	hypervisor*		
StartVirtualMachinesMetadataSync	授予权限 StartVirtualMachinesMetadataSync	写入	hypervisor*		iam:PassRole
TagResource	授予权限 TagResource	标记	gateway		
			hypervisor		
			virtualmachine		
				aws:RequestTag/${TagKey} aws:TagKeys	
TestHypervisorConfiguration	授予权限 TestHypervisorConfiguration	写入	gateway*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UntagResource	授予权限 UntagResource	标记	gateway		
			hypervisor		
			virtualmachine		
				aws:TagKeys	
UpdateGatewayInformation	授予权限 UpdateGatewayInformation	写入	gateway*		
UpdateGatewaySoftwareNow	授予权限 UpdateGatewaySoftwareNow	写入	gateway*		
UpdateHypervisor	授予权限 UpdateHypervisor	写入	gateway*		

Amazon Backup Gateway 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
gateway	arn:${Partition}:backup-gateway::${Account}:gateway/${GatewayId}	aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
hypervisor	arn:${Partition}:backup-gateway::${Account}:hypervisor/${HypervisorId}	aws:ResourceTag/${TagKey}
virtualmachine	arn:${Partition}:backup-gateway::${Account}:vm/${VirtualmachineId}	aws:ResourceTag/${TagKey}

Amazon Backup Gateway 的条件键

Amazon Backup Gateway 定义了以下可以在 IAM 策略Condition元素中使用的条件密钥。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按每个标签的允许值集筛选访问	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签值筛选访问权限	字符串
aws:TagKeys	按请求中是否具有必需标签来筛选访问	ArrayOfString

Amazon Backup 存储的操作、资源和条件键

Amazon Backup Storage（服务前缀:backup-storage）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon Backup 存储定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CommitBackupJob[仅权限]	授予权限以提交备份作业	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteObjects[仅权限]	授予权限以删除对象	写入			
DescribeBackupJob[仅权限]	授予权限以描述备份作业	写入			
GetBaseBackup[仅权限]	授予权限以获取基础备份	写入			
GetChunk[仅权限]	授予权限以为还原作业从恢复点获取数据	写入			
GetIncrementalBaseBackup[仅权限]	授予权限以获取增量基础备份	写入			
GetObjectMetadata[仅权限]	授予权限以为还原作业从恢复点获取元数据	写入			
ListChunks[仅权限]	授予权限以为还原作业从恢复点列出数据	写入			
ListObjects[仅权限]	授予权限以为还原作业从恢复点列出数据	写入			
MountCapsule[仅权限]	将 KMS 密钥与备份文件库关联	写入			
NotifyObjectComplete[仅权限]	授予权限以将备份作业的已上传数据标记为已完成	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutChunk[仅权限]	授予将数据上传到 Amazon 备份管理的恢复点以执行备份作业的权限	写入			
PutObject[仅权限]	授予权限以发送对象	写入			
StartObject[仅权限]	授予将数据上传到 Amazon 备份管理的恢复点以执行备份作业的权限	写入			
UpdateObjectComplete[仅权限]	授予权限以更新对象完成	写入			

Amazon Backup 存储定义的资源类型

Amazon Backup 存储不支持在 IAM 策略声明的`Resource`元素中指定资源 ARN。要允许对 Amazon Backup 存储的访问权限，请在策略中指定 `"Resource": "*"`。

Amazon Backup 存储的条件键

Backup 存储没有可在策略语句的 `Condition` 元素中使用的服务特定上下文键。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon Batch 的操作、资源和条件键

Amazon Batch（服务前缀:`batch`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon Batch 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CancelJob	授予取消您账户中 B Amazon atch 作业队列中任务的权限	写入	job*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateComputeEnvironment	授予在您的账户中创建 Amazon Batch 计算环境的权限	写入	compute-environment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConsumableResource	授予在您的账户中创建 Amazon Batch 可消耗资源的权限	写入	consumable-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateJobQueue	授予在您的账户中创建 Amazon Batch 作业队列的权限	写入	compute-environment*		
			job-queue*	aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			scheduling-policy		
CreateSchedulingPolicy	授予在您的账户中创建 Amazon Batch 计划策略的权限	写入	scheduling-policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteComputeEnvironment	授予删除您账户中的 Amazon Batch 计算环境的权限	写入	compute-environment*		
DeleteConsumableResource	授予删除您账户中 Amazon Batch 可消耗资源的权限	写入	consumable-resource*		
DeleteJobQueue	授予删除您账户中的 Amazon Batch 作业队列的权限	写入	job-queue*		
DeleteSchedulingPolicy	授予删除您账户中的 Amazon Batch 计划策略的权限	写入	scheduling-policy*		
DeregisterJobDefinition	授予在您的账户中注销 Amazon Batch 作业定义的权限	写入	job-definition-revision*		
DescribeComputeEnvironments	授予描述您账户中一个或多个 Amazon Batch 计算环境的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeConsumableResource	授予描述您账户中一个或多个 Amazon Batch 可消耗资源的权限	读取	consumable-resource*		
DescribeJobDefinitions	授予描述账户中一个或多个 B Amazon atch 作业定义的权限	读取			
DescribeJobQueues	授予描述您账户中一个或多个 Amazon Batch 作业队列的权限	读取			
DescribeJobs	授予描述您账户中的 B Amazon atch 任务列表的权限	读取			
DescribeSchedulingPolicies	授予描述您账户中一个或多个 Amazon Batch 调度策略的权限	读取			
GetJobQueueSnapshot	授予在您的账户中获取 B Amazon atch 作业队列快照的权限	读取	job-queue*		
ListConsumableResources	授予在您的账户中列 Amazon 出 Batch 可消耗资源的权限	列表			
ListJobs	授予在您的账户中列出指定 B Amazon atch 作业队列的任务的权限	列表			
ListJobsByConsumableResource	授予列出需要账户中特定消耗资源的 B Amazon atch 任务的权限	列表	consumable-resource*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListSchedulingPolicies	授予在您的账户中列 Amazon 出 Batch 计划策略的权限	读取			
ListTagsForResource	授予在您的账户中列出 Amazon Batch 资源标签的权限	读取	compute-environment		
			consumable-resource		
			job		
			job-definition-revision		
			job-queue		
			scheduling-policy		
RegisterJobDefinition	授予在您的账户中注册 Amazon Batch 作业定义的权限	写入	job-definition*		
			consumable-resource		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				batch:User batch:Privileged batch:Image batch:LogDriver batch:AWSLogsGroup batch:AWSLogsRegion batch:AWSLogsStreamPrefix batch:AWSLogsCreateGroup batch:EKSServiceAccountName batch:EKSImage batch:EKSRunAsUser	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				batch:EKSRunAsGroup batch:EKSPrivileged batch:EKSNamespace aws:RequestTag/${TagKey} aws:TagKeys	
SubmitJob	授予根据您账户中的任务定义提交 B Amazon atch 作业的权限	写入	job*	batch:ShareIdentifier batch:EKSImage batch:EKSNamespace aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			job-definition*		
			job-queue*		
			consumable-resource		
TagResource	授予在您的账户中为 Amazon Batch 资源添加标签的权限	标记	compute-environment		
			consumable-resource		
			job		
			job-definition-revision		
			job-queue		
			scheduling-policy		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
TerminateJob	授予终止您账户中 B Amazon atch 作业队列中任务的权限	写入	job*		
UntagResource	授予在您的账户中取消标记 Amazon Batch 资源的权限	标记	compute-environment		
			consumable-resource		
			job		
			job-definition-revision		
			job-queue		
			scheduling-policy		
				aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateComputeEnvironment	授予更新您账户中的 Amazon Batch 计算环境的权限	写入	compute-environment*		
UpdateConsumableResource	授予更新您账户中 Amazon Batch 可消耗资源的权限	写入	consumable-resource*		
UpdateJobQueue	授予更新您账户中的 Amazon Batch 作业队列的权限	写入	job-queue*		
			compute-environment		
			scheduling-policy		
UpdateSchedulingPolicy	授予更新您账户中的 Amazon Batch 计划策略的权限	写入	scheduling-policy*		

Amazon Batch 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}
consumable-resource	arn:${Partition}:batch:${Region}:${Account}:consumable-resource/${ConsumableResourceName}	aws:ResourceTag/${TagKey}

Amazon Batch 的条件键

Amazon Batch 定义了以下可在 IAM 策略Condition元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString
batch:AWSLogsCreateGroup	根据指定的日志记录驱动程序，筛选访问权限，以确定是否将为日志创建 awslog 组	布尔型
batch:AWSLogsGroup	根据日志所在的 awslog 组筛选访问权限	字符串
batch:AWSLogsRegion	根据日志发送到的区域筛选访问权限	字符串
batch:AWSLogsStreamPrefix	根据 awslog 日志流前缀筛选访问权限	字符串
batch:EKSImage	按用于启动 Amazon EKS 任务容器的映像筛选访问权限	字符串
batch:EKSNamespace	按用于为 Amazon EKS 作业运行 pod 的集群的命名空间筛选访问权限	字符串
batch:EKSPrivileged	按指定的特权参数值筛选访问权限，该参数值可确定是否为此容器提供了对 Amazon EKS 任务主机容器实例的提升权限（类似于根用户）	布尔型
batch:EKSRunAsGroup	按用于启动 Amazon EKS 任务中容器的指定组数字 ID（gid）筛选访问权限	数值

条件键	描述	类型
batch:EKSRunAsUser	按用于启动 Amazon EKS 任务中容器的指定用户数字 ID（uid）筛选访问权限	数值
batch:EKSServiceAccountName	按用于运行 Amazon EKS 任务容器组（pod）的服务账户名称筛选访问权限	字符串
batch:Image	按用于启动容器的映像筛选访问权限	字符串
batch:LogDriver	根据用于容器的日志驱动程序筛选访问权限	字符串
batch:Privileged	根据指定的特权参数值筛选访问权限，该参数值可确定是否为此容器提供了对主机容器实例的提升权限（类似于根用户）	布尔型
batch:ShareIdentifier	根据提交任务内使用的 shareIdentifier 筛选访问权限	字符串
batch:User	根据容器内使用的用户名或数字 UID 筛选访问权限	字符串

Amazon Billing的操作、资源和条件键

Amazon Billing （服务前缀:`billing`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Billing定义的操作
- Amazon Billing定义的资源类型
- Amazon Billing的条件键

Amazon Billing定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateBillingView	授予创建账单视图的权限	写入	billingview*		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteBillingView	授予删除账单视图的权限	写入	billingview*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy[仅权限]	授予删除账单视图资源策略的权限	权限管理	billingview*		
				aws:ResourceTag/${TagKey}	
GetBillingData[仅权限]	授予对账单信息执行查询的权限	读取			
GetBillingDetails[仅权限]	授予查看详细行项目账单信息的权限	读取			
GetBillingNotifications[仅权限]	授予权限以查看由您发送的 Amazon 与您的账户账单信息相关的通知	读取			
GetBillingPreferences[仅权限]	授予查看账单首选项的权限，例如预留实例、实惠配套和服务抵扣金共享	读取			
GetBillingView	授予获取指定账单视图元数据的权限	读取	billingview*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey}	
GetContractInformation[仅权限]	授予查看账户合同信息的权限，包括合同编号、最终用户组织名称、采购订单号，以及账户是否用于为公共部门客户提供服务	读取			
GetCredits[仅权限]	授予查看已兑换的服务抵扣金的权限	读取			
GetIAMAccessPreference[仅权限]	授予检索“允许 IAM 访问”账单首选项的状态的权限	读取			
GetResourcePolicy	授予权限以获取资源策略指定的账单视图	权限管理	billingview*		
				aws:ResourceTag/${TagKey}	
GetSellerOfRecord[仅权限]	授予检索账户的默认记录卖家的权限	读取			
ListBillingViews	授予获取所有可用账单视图列表的权限	读取			
ListSourceViewsForBillingView	授予获取指定账单视图的源视图列表的权限	列表	billingview*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey}	
ListTagsForResource	授予获取指定账单视图的标签列表的权限	读取	billingview*		
				aws:ResourceTag/${TagKey}	
PutContractInformation[仅权限]	授予设置账户合同信息、最终用户组织名称，以及账户是否用于为公共部门客户提供服务的权限	写入			
PutResourcePolicy[仅权限]	授予制定账单视图资源政策的权限	权限管理	billingview*		
				aws:ResourceTag/${TagKey}	
RedeemCredits[仅权限]	授予兑换积分的 Amazon 权限	写入			
TagResource	授予向指定账单视图添加标签的权限	标记	billingview*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	授予从指定账单视图中移除标签的权限	标记	billingview*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateBillingPreferences[仅权限]	授予更新账单首选项的权限，例如预留实例、实惠配套和服务抵扣金共享	写入			
UpdateBillingView	授予更新账单视图的权限	写入	billingview*		
				aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateIAMAccessPreference[仅权限]	授予更新“允许 IAM 访问”账单首选项的权限	写入			

Amazon Billing定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
billingview	arn:${Partition}:billing::${Account}:billingview/${ResourceId}	aws:ResourceTag/${TagKey}

Amazon Billing的条件键

Amazon Billing 定义了可在 IAM 策略Condition元素中使用的以下条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串

条件键	描述	类型
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString

Amazon Billing 控制台的操作、资源和条件键

Amazon Billing 控制台（服务前缀:aws-portal）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- 由 Amazon Billing 控制台定义的操作
- 由 Amazon Billing 控制台定义的资源类型
- Amazon Billing 控制台的条件键

由 Amazon Billing 控制台定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetConsoleActionSetEnforced[仅权限]	授予权限以查看是否使用现有或精细的 IAM 操作来控制对账单、成本管理和账户控制台的授权	读取			
ModifyAccount[仅权限]	允许或拒绝 IAM 用户修改账户设置的权限	写入			
ModifyBilling[仅权限]	允许或拒绝 IAM 用户修改账单设置的权限	写入			
ModifyPaymentMethods[仅权限]	允许或拒绝 IAM 用户修改付款方式的权限	写入			
UpdateConsoleActionSetEnforced[仅权限]	授予权限以更改是使用现有还是精细的 IAM 操作来控制对账单、成本管理和账户控制台的授权	写入			
ViewAccount[仅权限]	允许或拒绝 IAM 用户查看账户设置的权限	读取			
ViewBilling[仅权限]	允许或拒绝 IAM 用户在控制台中查看账单页面的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ViewPaymentMethods[仅权限]	允许或拒绝 IAM 用户查看付款方式的权限	读取			
ViewUsage[仅权限]	允许或拒绝 IAM 用户查看 Amazon 使用情况报告的权限	读取			

由 Amazon Billing 控制台定义的资源类型

Amazon Billing 控制台不支持在 IAM 策略声明的`Resource`元素中指定资源 ARN。要允许对 Amazon Billing 控制台的访问权限，请在策略中指定 `"Resource": "*"`。

Amazon Billing 控制台的条件键

账单控制台没有可在策略语句的 `Condition` 元素中使用的服务特定上下文键。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon Budget Service 的操作、资源和条件键

Amazon Budget Service（服务前缀:`budgets`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Budget Service 定义的操作
- Amazon Budget Service 定义的资源类型
- Amazon Budget Service 的条件键

Amazon Budget Service 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

> **Note**
>
> 此表中的操作不是 APIs，而是授予访问权限预算 Amazon Billing and Cost Management APIs 的权限。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateBudgetAction	授予权限以配置响应，该响应在预算超出特定的预算阈值后执行。创建带有标签的预	写入	budgetAction*		iam:PassRole

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
	算操作还需要 “预算：TagResource” 权限			aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteBudgetAction	授予权限以删除与特定预算关联的操作	写入	budgetAction*		
DescribeBudgetAction	授予权限以检索与预算关联的特定预算操作的详细信息	读取	budgetAction*		
DescribeBudgetActionHistories	授予权限以检索与特定预算操作关联的预算操作状态的历史视图 这些状态包括“待机”、“待定”和“已执行”等状态	读取	budgetAction*		
DescribeBudgetActionsForAccount	授予权限以检索与您的账户关联的所有预算操作的详细信息	读取			
DescribeBudgetActionsForBudget	授予权限以检索与预算关联的所有预算操作的详细信息	读取	budget*		
ExecuteBudgetAction	授予权限以启动待定的预算操作以及撤销先前执行的预算操作	写入	budgetAction*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListTagsForResource	授予权限以查看预算或预算操作的资源标签	读取	budget		
			budgetAction		
ModifyBudget	授予权限以创建和修改预算，以及编辑预算详细信息。创建带有标签的预算还需要 “预算：TagResource” 权限	写入	budget*		
TagResource	授予权限以将资源标签应用于预算或预算操作。还需要创建带标签的预算或预算操作	标记	budget		
			budgetAction		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	授予权限以从预算或预算操作中删除标签	标记	budget		
			budgetAction		
				aws:TagKeys	
UpdateBudgetAction	授予权限以更新与预算关联的特定预算操作的详细信息	写入	budgetAction*		iam:PassRole
ViewBudget	授予权限以查看预算和预算详细信息	读取	budget*		

Amazon Budget Service 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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

Amazon Budget Service 的条件键

Amazon 预算服务定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中传递的标签筛选访问	字符串

条件键	描述	类型
aws:ResourceTag/${TagKey}	根据与资源关联的标签筛选访问	字符串
aws:TagKeys	根据在请求中传递的标签键筛选访问	ArrayOfString

Amazon Certificate Manager 的操作、资源和条件键

Amazon Certifice Manager（服务前缀:acm）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Certificate Manager 定义的操作
- Amazon Certificate Manager 定义的资源类型
- Amazon Certificate Manager 的条件键

Amazon Certificate Manager 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddTagsToCertificate	授予权限以将一个或多个标签添加到证书中	Tagging	certificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCertificate	授予权限以删除证书及其关联的私有密钥	Write	certificate*		
DescribeCertificate	授予权限以检索证书及其元数据	Read	certificate*		
ExportCertificate	授予权限以导出私有证书颁发机构 (CA) 颁发的私有证书以在任何位置中使用	读取	certificate*		
GetAccountConfiguration	授予从 Certifice Manager Amazon 检索账户级别配置的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetCertificate	授予权限以检索证书 ARN 的证书和证书链	读取	certificate*		
ImportCertificate	授予将第三方证书导入到 Certifice Manager (ACM) 的权限 Amazon	写入	certificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListCertificates	授予检索每个 ARN 的证书列表 ARNs 和域名的权限	列表			
ListTagsForCertificate	授予权限以列出与证书关联的标签	读取	certificate*		
PutAccountConfiguration	授予在 Certifice Manager 中更新账户级别 Amazon 配置的权限	写入			
RemoveTagsFromCertificate	授予权限以从证书删除一个或多个标签	Tagging	certificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RenewCertificate	授予权限以续订符合条件的私有证书	Write	certificate*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
RequestCertificate	授予权限以申请公有或私有证书	Write		aws:RequestTag/${TagKey} aws:TagKeys acm:DomainNames acm:CertificateTransparencyLogging acm:ValidationMethod acm:KeyAlgorithm acm:CertificateAuthority	
ResendValidationEmail	授予权限以重新发送电子邮件以请求验证域所有权	Write	certificate*		
UpdateCertificateOptions	授予权限以更新证书配置 使用此选项指定是选择加入还是退出证书透明度日志记录	写入	certificate*		

Amazon Certificate Manager 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
certificate	arn:${Partition}:acm:${Region}:${Account}:certificate/${CertificateId}	aws:ResourceTag/${TagKey}

Amazon Certificate Manager 的条件键

Amazon Certifice Manager 定义了以下可以在 IAM 策略Condition元素中使用的条件密钥。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
acm:CertificateAuthority	按请求中的 certificateAuthority 筛选访问权限。可用于限制可以从哪些证书颁发机构颁发证书	字符串
acm:CertificateTransparencyLogging	按请求中的 certificateTransparencyLogging 选项筛选访问权限。如果请求中没有密钥，则默认为“ENABLED”	字符串
acm:DomainNames	按请求中的 domainNames 筛选访问权限 此密钥可用于限制证书请求中可以包含哪些域	ArrayOfString
acm:KeyAlgorithm	按请求中的 keyAlgorithm 筛选访问权限	字符串
acm:ValidationMethod	按请求中的 validationMethod 筛选访问权限 如果请求中没有密钥，则默认为“EMAIL”	字符串

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对来筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按附加到资源的标签键值对筛选操作	字符串
aws:TagKeys	根据在请求中是否具有标签键来筛选访问	ArrayOfString

Amazon Web Services 云 Map 的操作、资源和条件键

Amazon Web Services 云 Map（服务前缀:`servicediscovery`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Web Services 云 Map 定义的操作
- Amazon Web Services 云 Map 定义的资源类型
- Amazon Web Services 云 Map 的条件键

Amazon Web Services 云 Map 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须

具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateHttpNamespace	授予创建 HTTP 命名空间的权限	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreatePrivateDnsNamespace	授予根据 DNS 创建私有命名空间（仅在指定的 Amazon VPC 内才可见）的权限	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreatePublicDnsNamespace	授予根据 DNS 创建公有命名空间（在 Internet 上可见）的权限	Write		aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey}	
CreateService	授予创建服务的权限	Write	namespace*		
			service*		
				servicediscovery:NamespaceArn aws:TagKeys aws:RequestTag/${TagKey}	
DeleteNamespace	授予删除指定命名空间的权限	Write	namespace*		
DeleteService	授予删除指定服务的权限	写入	service*		
DeleteServiceAttributes	授予从服务中删除指定属性的权限	写入	service*		
DeregisterInstance	授予删除 Amazon Route 53 为指定实例创建的记录和运行状况检查的权限（如果有）	Write	service*		
				servicediscovery:ServiceArn	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DiscoverInstances	授予为指定命名空间和服务发现注册实例的权限	读取		servicediscovery:NamespaceName servicediscovery:ServiceName	
DiscoverInstancesRevision	授予为指定的命名空间和服务发现实例修订的权限	读取		servicediscovery:NamespaceName servicediscovery:ServiceName	
GetInstance	授予获取有关指定实例的信息的权限	Read		servicediscovery:ServiceArn	
GetInstancesHealthStatus	授予获取一个或多个实例的当前运行状况（正常、不正常或未知）的权限	Read		servicediscovery:ServiceArn	
GetNamespace	授予获取有关命名空间信息的权限	Read	namespace*		
GetOperation	授予获取有关指定操作信息的权限	Read			
GetService	授予获取指定服务设置的权限	读取	service*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetServiceAttributes	授予获取指定服务属性的权限	读取	service*		
ListInstances	授予权限，以获取在指定服务中注册的实例的相关摘要信息	读取		servicediscovery:ServiceArn	
ListNamespaces	授予获取有关命名空间信息的权限	读取			
ListOperations	授予列出与指定条件匹配的操作的权限	List			
ListServices	授予获取与指定筛选条件匹配的所有服务的设置的权限	读取			
ListTagsForResource	授予为指定资源列出标签的权限	读取			
RegisterInstance	授予根据指定服务中的设置注册实例的权限	Write	service*		
				servicediscovery:ServiceArn	
TagResource	授予将一个或多个标签添加到指定资源的权限	Tagging		aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	授予从指定资源中删除一个或多个标签的权限	标记		aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateHttpNamespace	授予权限以更新 HTTP 命名空间的设置	写入	namespace*		
UpdateInstanceCustomHealthStatus	授予权限以更新具有自定义运行状况检查的实例的当前健康状态	写入		servicediscovery:ServiceArn	
UpdatePrivateDnsNamespace	授予权限以更新私有 DNS 命名空间的设置	写入	namespace*		
UpdatePublicDnsNamespace	授予权限以更新公有 DNS 命名空间的设置	写入	namespace*		
UpdateService	授予更新指定服务中设置的权限	写入	service*		
UpdateServiceAttributes	授予更新指定服务中属性的权限	写入	service*		

Amazon Web Services 云 Map 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
namespace	arn:${Partition}:servicediscovery:${Region}:${Account}:namespace/${NamespaceId}	aws:ResourceTag/${TagKey}
service	arn:${Partition}:servicediscovery:${Region}:${Account}:service/${ServiceId}	aws:ResourceTag/${TagKey}

Amazon Web Services 云 Map 的条件键

Amazon Web Services 云 Map 定义了可在 IAM 策略Condition元素中使用的以下条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中传递的标签筛选操作	字符串
aws:ResourceTag/${TagKey}	根据与资源关联的标签筛选操作	字符串
aws:TagKeys	根据在请求中传递的标签键筛选操作	ArrayOfString
servicediscovery:NamespaceArn	通过为相关命名空间指定 Amazon Resource Name (ARN) 来筛选访问权限	ARN
servicediscovery:NamespaceName	通过指定相关命名空间的名称来筛选访问权限	字符串

条件键	描述	类型
servicediscovery:ServiceArn	通过为相关服务指定 Amazon Resource Name (ARN) 来筛选访问权限	ARN
servicediscovery:ServiceName	通过指定相关服务的名称来筛选访问权限	字符串

Amazon CloudAssist 服务读写权限的操作、资源和条件密钥

Amazon CloudAssist 服务读写权限（服务前缀:`cloudassist`）提供以下特定于服务的资源、操作和条件上下文密钥以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- 由 Amazon CloudAssist 服务读写权限定义的操作
- 由 Amazon CloudAssist 服务读写权限定义的资源类型
- Amazon CloudAssist 服务读写权限的条件密钥

由 Amazon CloudAssist 服务读写权限定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用

Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeAccountRealNameInformation	授予获取账户实名信息的权限	读取			
UpdateAccountRealNameInformation	授予更新账户实名信息的权限	写入			

由 Amazon CloudAssist 服务读写权限定义的资源类型

Amazon CloudAssist 服务读写权限不支持在 IAM 策略声明的Resource元素中指定资源 ARN。要允许访问 Amazon CloudAssist 服务的读写权限，请在策略"Resource": "*"中指定。

Amazon CloudAssist 服务读写权限的条件密钥

CloudAssist 没有可在策略声明Condition元素中使用的特定于服务的上下文密钥。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon CloudFormation 的操作、资源和条件键

Amazon CloudFormation （服务前缀:cloudformation）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon CloudFormation 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ActivateOrganizationsAccess	授予在和 Organizations StackSets 之间激活可信访问的权限。激活 StackSets 和 Organizations 之间的可信访问权限后，管理账户有权 StackSets 为您的组织创建和管理	写入			
ActivateType	授予权限以激活公有第三方扩展，使其可用于堆栈模板	写入			
BatchDescribeTypeConfigurations	授予返回指定 CloudFormation 扩展程序配置数据的权限	读取			
CancelUpdateStack	授予权限以取消指定堆栈更新	Write	stack*		
ContinueUpdateRollback	授予继续将处于 UPDATE_ROLLBACK_FAILED 状态的堆栈回滚到 UPDATE_ROLLBACK_COMPLETE 状态的权限	Write	stack*		
				cloudformation:RoleArn	
CreateChangeSet	授予为堆栈创建更改列表的权限	写入	stack*		
				cloudformation:ChangeSetName cloudformation:Res	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				ourceTypes cloudformation:ImportResourceTypes cloudformation:RoleArn cloudformation:StackPolicyUrl cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	
CreateGeneratedTemplate	授予使用尚未管理的现有资源创建模板的权限 CloudFormation	写入			
CreateStack	授予依照模板中的指定创建堆栈的权限	Write	stack*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				cloudformation:ResourceTypes cloudformation:RoleArn cloudformation:StackPolicyUrl cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	
CreateStackInstances	授予在指定区域内为指定账户创建堆栈实例的权限	写入	stackset*		
			stackset-target		
			type		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys cloudformation:TargetRegion	
CreateStackRefactor	授予创建堆栈重构的权限	写入	stack*		
CreateStackSet	授予依照模板中的指定创建堆栈集的权限	Write		cloudformation:RoleArn cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	
CreateUploadBucket[仅权限]	授予将模板上传到 Amazon S3 存储桶的权限。仅供 Amazon CloudFormation 控制台使用，未记录在 API 参考中	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeactivateOrganizationsAccess	授予在和 Organizations 之间停用可信访问权限 StackSets 的权限。如果停用可信访问权限，则该管理账户无权为您的组织创建和管理服务托管服务 StackSets	写入			
DeactivateType	授予权限以停用先前在此账户和区域中激活的公有扩展	写入			
DeleteChangeSet	授予删除指定更改集的权限。删除更改集可确保没有人执行错误的更改集	写入	stack*		
				cloudformation:ChangeSetName	
DeleteGeneratedTemplate	授予权限以删除生成的模板	写入			
DeleteStack	授予删除指定堆栈的权限	Write	stack*		
				cloudformation:RoleArn	
DeleteStackInstances	授予在指定区域内删除指定账户的堆栈实例的权限	Write	stackset*		
			stackset-target		
			type		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				cloudformation:TargetRegion	
DeleteStackSet	授予删除指定堆栈集的权限	写入	stackset*		
DeregisterType	授予取消注册现有 CloudFormation 类型或类型版本的权限	写入			
DescribeAccountLimits	授予权限以检索您的账户 Amazon CloudFormation 限额	读取			
DescribeChangeSet	授予返回指定更改集的描述的权限	读取	stack*		
				cloudformation:ChangeSetName	
DescribeChangeSetHooks	授予返回指定更改集的 Hook 调用信息的权限	读取	stack*		
				cloudformation:ChangeSetName	
DescribeGeneratedTemplate	授予权限以描述生成的模板 输出包括有关生成模板的创建进度的详细信息	读取			
DescribeOrganizationsAccess	授予返回有关账户 OrganizationAccess 状态信息的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribePublisher	授予返回 CloudFormation 扩展发布者相关信息的权限	读取			
DescribeResourceScan	授予权限以描述资源扫描的详细信息	读取			
DescribeStackDriftDetectionStatus	授予返回有关堆栈偏差检测操作的信息的权限	Read			
DescribeStackEvents	授予为指定堆栈返回所有与堆栈相关事件的权限	读取	stack*		
DescribeStackInstance	授予返回与指定堆栈集 Amazon Web Services 账户、和区域关联的堆栈实例的权限	读取	stackset*		
DescribeStackRefactor	授予返回指定堆栈重构描述的权限	读取	stack*		
DescribeStackResource	授予返回指定堆栈中指定资源描述的权限	Read	stack*		
DescribeStackResourceDrifts	授予返回已针对指定堆栈中的偏差进行检查的资源偏差信息的权限	读取	stack*		
DescribeStackResources	授予返回正在运行的堆栈和已删除堆栈的 Amazon 资源描述的权限	读取	stack*		
DescribeStackSet	授予返回指定堆栈集描述的权限	Read	stackset*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeStackSetOperation	授予返回指定堆栈集操作描述的权限	读取	stackset*		
DescribeStacks	授予返回指定堆栈描述的权限，以及与操作结合使用时返回所有堆栈的描述的 ListStacks 权限	列表	stack		cloudformation:ListStacks
DescribeType	授予返回有关所请求 CloudFormation 类型信息的权限	读取			
DescribeTypeRegistration	授予返回有关 CloudFormation 类型注册过程信息的权限	读取			
DetectStackDrift	授予权限，以检测堆栈的实际配置是否与预期配置（在堆栈模板以及指定为模板参数的任何值中定义）不同或出现偏差	Read	stack*		
DetectStackResourceDrift	授予权限，以返回有关资源的实际配置是否与预期配置（在堆栈模板以及指定为模板参数的任何值中定义）不同或出现偏差的信息	Read	stack*		
DetectStackSetDrift	授予权限，使用户能够检测堆栈集以及属于该堆栈集的堆栈实例上的偏差	Read	stackset*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
EstimateTemplateCost	授予返回模板每月估计成本的权限	Read		cloudformation:TemplateUrl	
ExecuteChangeSet	授予创建指定更改集时使用提供的输入信息更新堆栈的权限	写入	stack*		
				cloudformation:ChangeSetName	
ExecuteStackRefactor	授予使用创建指定堆栈重构时提供的输入信息执行堆栈重构的权限	写入	stack*		
GetGeneratedTemplate	授予权限以检索生成的模板	读取			
GetStackPolicy	授予为指定堆栈返回堆栈策略的权限	Read	stack*		
GetTemplate	授予为指定堆栈返回模板正文的权限	Read	stack*		
GetTemplateSummary	授予返回有关新模板或现有模板信息的权限	读取	stack		
			stackset		
				cloudformation:TemplateUrl	
ImportStacksToStackSet	授予允许用户将现有堆栈导入到新堆栈或现有堆栈集的权限	写入	stackset*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListChangeSets	授予权限以返回堆栈的每个活动更改集的 ID 和状态。例如，Amazon CloudFormation 列出处于 CREATE_IN_PROGRESS 或 CREATE_PENDING 状态的更改集	列表	stack*		
ListExports	授予权限，以列出您在其中调用此操作的账户和区域中的所有已导出输出值	列表			
ListGeneratedTemplates	授予权限以列出您在该区域生成的模板	列表			
ListHookResults	授予返回指定目标的 Hook 调用结果信息的权限	列表	stack		
				cloudformation:ChangeSetName	
ListImports	授予列出导出输出值的所有堆栈的权限	列表			
ListResourceScanRelatedResources	授予权限以列出资源扫描中资源列表的相关资源。该响应表明每个返回的资源是否已由管理 CloudFormation	列表			
ListResourceScanResources	授予权限以列出资源扫描中的资源。可以按资源标识符、资源类型前缀、标签键和标签值筛选结果	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListResourceScans	授予权限以从最新到最旧列出资源扫描。默认情况下，它将返回最多 10 次资源扫描	列表			
ListStackInstanceResourceDrifts	授予返回已针对指定堆栈实例中偏差进行检查的资源偏差信息的权限	列表	stackset*		
ListStackInstances	授予权限，以返回与指定堆栈集关联的相关堆栈实例的摘要信息	列表	stackset*		
ListStackRefactorActions	授予返回指定堆栈重构操作列表的权限	列表	stack*		
ListStackRefactors	授予返回每个活动堆栈重构的 ID 和状态的权限	列表	stack*		
ListStackResources	授予返回指定堆栈中所有资源描述的权限	列表	stack*		
ListStackSetAutoDeploymentTargets	授予返回有关 StackSet 自动部署目标的摘要信息的权限	列表	stackset*		
ListStackSetOperationResults	授予返回有关堆栈集操作结果的摘要信息的权限	List	stackset*		
ListStackSetOperations	授予返回有关堆栈集上执行操作的摘要信息的权限	List	stackset*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListStackSets	授予返回与用户关联的堆栈集的摘要信息的权限	列表			
ListStacks	授予返回状态与指定值StackStatusFilter匹配的堆栈摘要信息的权限。与 DescribeStacks 操作相结合，授予列出堆栈描述的权限	列表			
ListTypeRegistrations	授予列出 CloudFormation 类型注册尝试次数的权限	列表			
ListTypeVersions	授予列出特定 CloudFormation 类型版本的权限	列表			
ListTypes	授予列出可用 CloudFormation 类型的权限	列表			
PublishType	授予将指定扩展作为该区域的公共扩展发布到 CloudFormation 注册表的权限	写入			
RecordHandlerProgress	授予权限以记录处理程序进度	写入	stack*		
RegisterPublisher	授予在注册 CloudFormation 表中将账户注册为公共扩展发布者的权限	写入			
RegisterType	授予注册新 CloudFormation 类型的权限	写入			
RollbackStack	授予将堆栈回滚到最后一个稳定状态的权限	写入	stack*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				cloudformation:RoleArn	
SetStackPolicy	授予为指定堆栈设置堆栈策略的权限	权限管理	stack*		
				cloudformation:StackPolicyUrl	
SetTypeConfiguration	授予在给定账户和区域中为已注册的 CloudFormation 扩展程序设置配置数据的权限	写入			
SetTypeDefaultVersion	授予权限以设置某一 CloudFormation 类型的哪个版本适用于 CloudFormation 操作	写入			
SignalResource	授予向指定资源发送包含成功或失败状态信号的权限	写入	stack*		
StartResourceScan	授予权限以开始扫描该账户在该区域的资源	写入			
StopStackSetOperation	授予停止对堆栈集及其关联堆栈实例的进行中操作的权限	Write	stackset*		
TagResource	授予标记 CloudFormation 资源的权限	标记	changeset		
			stack		
			stackset		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys aws:RequestTag/${TagKey} cloudformation:CreateAction	
TestType	授予测试已注册扩展程序的权限，以确保其满足在 CloudFormation 注册表中发布的所有必要要求	写入			
UntagResource	授予权限以取消标记 CloudFormation 资源	标记	changeset		
			stack		
			stackset		
				aws:TagKeys cloudformation:CreateAction	
UpdateGeneratedTemplate	授予权限以更新生成的模板 这可用于更改名称、添加和删除资源、刷新资源以及更改 DeletionPolicy 和 UpdateReplacePolicy 设置	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateStack	授予依照模板中的指定更新堆栈的权限	Write	stack*		
				cloudformation:ResourceTypes cloudformation:RoleArn cloudformation:StackPolicyUrl cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	
UpdateStackInstances	授予在指定区域内为指定账户的堆栈实例更新参数值的权限。	Write	stackset*		
			stackset-target		
			type		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				cloudformation:TargetRegion	
UpdateStackSet	授予依照模板中的指定更新堆栈集的权限	Write	stackset*		
			stackset-target		
			type		
				cloudformation:RoleArn cloudformation:TemplateUrl cloudformation:TargetRegion aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTerminationProtection	授予为指定堆栈更新终止保护的权限	Write	stack*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ValidateTemplate	授予验证指定模板的权限	读取		cloudformation:TemplateUrl	

Amazon CloudFormation 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}	
type	arn:${Partition}:cloudformation:${Region}:${Account}:type/resource/${Type}	

资源类型	ARN	条件键
generated template	arn:${Partition}:cloudformation:${Region}:${Account}:generatedTemplate/${Id}	
resources can	arn:${Partition}:cloudformation:${Region}:${Account}:resourceScan/${Id}	

Amazon CloudFormation 的条件键

Amazon CloudFormation 定义了可在 IAM 策略Condition元素中使用的以下条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString
cloudformation:ChangeSetName	按 Amazon CloudFormation 更改集名称筛选访问权限。用于控制 IAM 用户可执行或删除的更改集	字符串
cloudformation:CreateAction	按资源变更的 API 操作的名称筛选访问权限。用于控制哪些 APIs IAM 用户可以使用在堆栈或堆栈集上添加或删除标签	字符串
cloudformation:Imp	按模板资源类型筛选访问权限，例如 Amazon::EC2:Instance。用于控制 IAM 用户希望将资源导入堆栈时可以使用的资源类型	字符串

条件键	描述	类型
ortResourceTypes		
cloudformation:ResourceTypes	按模板资源类型筛选访问权限，例如 Amazon::EC2:Instance。用于控制 IAM 用户在创建或更新堆栈时可以使用的资源类型	ArrayOfString
cloudformation:RoleArn	按 IAM 服务角色的 ARN 筛选访问权限。用于控制 IAM 用户在处理堆栈或更改集时可使用的服务角色	ARN
cloudformation:StackPolicyUrl	按 Amazon S3 堆栈策略 URL 筛选访问权限。用于控制在创建或更新堆栈操作期间 IAM 用户可将哪些堆栈策略关联到堆栈	字符串
cloudformation:TargetRegion	按堆栈集目标区域筛选访问权限。用于控制 IAM 用户在创建或更新堆栈集时可以使用的区域	ArrayOfString
cloudformation:TemplateUrl	按 Amazon S3 模板 URL 筛选访问权限。用于控制 IAM 用户在创建或更新堆栈时可以使用的模板	字符串

Amazon 的操作、资源和条件密钥 CloudFront

Amazon CloudFront （服务前缀:`cloudfront`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon 定义的操作 CloudFront

- Amazon 定义的资源类型 CloudFront
- Amazon 的条件密钥 CloudFront

Amazon 定义的操作 CloudFront

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AllowVendedLogDeliveryForResource[仅权限]	授予为分发配置供给日志传输的权限	权限管理	distribution		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateAlias	授予将别名关联到 CloudFront 分配的权限	写入	distribution*		
CopyDistribution	授予复制现有分发和创建新 Web 分发的权限	写入	distribution*		cloudfront:CopyDistribution cloudfront:CreateDistribution cloudfront:GetDistribution
CreateAnycastIpList	授予创建 Anycast 静态 IP 列表的权限	写入	anycast-ip-list*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCachePolicy	授予向添加新缓存策略的权限 CloudFront	写入	cache-policy*		
CreateCloudFrontOriginAccessIdentity	授予创建新 CloudFront 源访问身份的权限	写入	origin-access-identity*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateContinuousDeploymentPolicy	授予向添加新的持续部署策略的权限 CloudFront	写入	continuous-deployment-policy*		
CreateDistribution	授予权限以创建新 Web 分配	写入	distribution*		
CreateFieldLevelEncryptionConfig	授予权限以创建新的字段级加密配置	Write			
CreateFieldLevelEncryptionProfile	授予权限以创建字段级加密配置文件	写入			
CreateFunction	授予创建 CloudFront 函数的权限	写入	function*		
CreateInvalidation	授予权限以创建新的失效批处理请求	写入	distribution*		
CreateKeyGroup	授予向其添加新密钥组的权限 CloudFront	写入			
CreateKeyValueStore	授予创建 CloudFront KeyValueStore	写入	key-value-store*		
CreateMonitoringSubscription	授予为指定 CloudFront 分配启用其他 CloudWatch 指标的权限。额外指标会产生额外费用	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateOriginAccessControl	授予权限以创建新的源访问控制	写入			
CreateOriginRequestPolicy	授予向添加新的起源请求策略的权限 CloudFront	写入	origin-request-policy*		
CreatePublicKey	授予向添加新公钥的权限 CloudFront	写入			
CreateRealtimeLogConfig	授予权限以创建实时日志配置	写入	realtime-log-config*		
CreateResponseHeadersPolicy	授予向添加新的响应标头策略的权限 CloudFront	写入	response-headers-policy*		
CreateSavingsPlan[仅权限]	授予权限以创建新的 Savings Plan	写入			
CreateStreamingDistribution	授予权限以创建新 RTMP 分配	Write	streaming-distribution*		
CreateStreamingDistributionWithTags	授予权限以创建带标签的新 RTMP 分配	写入	streaming-distribution*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVpcOrigin	授予创建 VPC 源的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAnycastIpList	授予删除 Anycast 静态 IP 列表的权限	写入	anycast-ip-list*		
DeleteCachePolicy	授予权限以删除缓存策略	写入	cache-policy*		
DeleteCloudFrontOriginAccessIdentity	授予删除 CloudFront 源访问身份的权限	写入	origin-access-identity*		
DeleteContinuousDeploymentPolicy	授予删除持续部署策略的权限	写入	continuous-deployment-policy*		
DeleteDistribution	授予权限以删除 Web 分配	Write	distribution*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteFieldLevelEncryptionConfig	授予权限以删除字段级加密配置	Write	field-level-encryption-config*		
DeleteFieldLevelEncryptionProfile	授予权限以删除字段级加密配置文件	写入	field-level-encryption-profile*		
DeleteFunction	授予删除 CloudFront 函数的权限	写入	function*		
DeleteKeyGroup	授予权限以删除密钥组	写入			
DeleteKeyValueStore	授予删除权限 CloudFront KeyValueStore	写入	key-value-store*		
DeleteMonitoringSubscription	授予禁用指定 CloudFront 分布的其他 CloudWatch 指标的权限	写入			
DeleteOriginAccessControl	授予权限以删除源访问控制	写入	origin-access-control*		
DeleteOriginRequestPolicy	授予权限以删除源请求策略	写入	origin-request-policy*		
DeletePublicKey	授予从中删除公钥的权限 CloudFront	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteRealtimeLogConfig	授予权限以删除实时日志配置	写入	realtime-log-config*		
DeleteResponseHeadersPolicy	授予权限以删除响应标头策略	写入	response-headers-policy*		
DeleteStreamingDistribution	授予权限以删除 RTMP 分配	写入	streaming-distribution*		
DeleteVpcOrigin	授予删除 VPC 源的权限	写入	vpcorigin*		
DescribeFunction	授予获取 CloudFront 函数摘要的权限	读取	function*		
DescribeKeyValueStore	授予获取 CloudFront KeyValueStore 摘要的权限	读取	key-value-store*		
GetAnycastIpList	授予获取 Anycast 静态 IP 列表的权限	读取	anycast-ip-list*		
GetCachePolicy	授予权限以获取缓存策略	Read	cache-policy*		
GetCachePolicyConfig	授予权限以获取缓存策略配置	读取	cache-policy*		
GetCloudFrontOriginAccessIdentity	授予获取有关 CloudFront 源访问身份信息的权限	读取	origin-access-identity*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetCloudFrontOriginAccessIdentityConfig	授予权限以获取有关 CloudFront 来源访问标识 (OAI) 配置信息	读取	origin-access-identity*		
GetContinuousDeploymentPolicy	授予获取持续部署策略的权限	读取	continuous-deployment-policy*		
GetContinuousDeploymentPolicyConfig	授予获取持续部署策略配置的权限	读取	continuous-deployment-policy*		
GetDistribution	授予权限以获取有关 Web 分配信息	Read	distribution*		
GetDistributionConfig	授予权限以获取有关分配的配置信息	Read	distribution*		
GetFieldLevelEncryption	授予权限以获取字段级加密配置信息	Read	field-level-encryption-config*		
GetFieldLevelEncryptionConfig	授予权限以获取字段级加密配置信息	Read	field-level-encryption-config*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetFieldLevelEncryptionProfile	授予权限以获取字段级加密配置信息	Read	field-level-encryption-profile*		
GetFieldLevelEncryptionProfileConfig	授予权限以获取字段级加密配置文件配置信息	读取	field-level-encryption-profile*		
GetFunction	授予获取 CloudFront 函数代码的权限	读取	function*		
GetInvalidation	授予权限以获取有关失效的信息	Read	distribution*		
GetKeyGroup	授予权限以获取密钥组	Read			
GetKeyGroupConfig	授予权限以获取密钥组配置	读取			
GetMonitoringSubscription	授予权限以获取有关是否为指定 CloudFront 分配启用了其他 CloudWatch 指标的信息	读取			
GetOriginAccessControl	授予权限以获取源访问控制	读取	origin-access-control*		
GetOriginAccessControlConfig	授予权限以获取源访问控制配置	读取	origin-access-control*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetOriginRequestPolicy	授予权限以获取源请求策略	Read	origin-request-policy*		
GetOriginRequestPolicyConfig	授予权限以获取源请求策略配置	Read	origin-request-policy*		
GetPublicKey	授予权限以获取公有密钥信息	Read			
GetPublicKeyConfig	授予权限以获取公有密钥配置信息	Read			
GetRealtimeLogConfig	授予权限以获取实时日志配置	读取	realtime-log-config*		
GetResponseHeadersPolicy	授予权限以获取响应标头策略	读取	response-headers-policy*		
GetResponseHeadersPolicyConfig	授予权限以获取响应标头策略配置	读取	response-headers-policy*		
GetSavingsPlan[仅权限]	授予权限以获取 Savings Plan	读取			
GetStreamingDistribution	授予权限以获取有关 RTMP 分配信息	Read	streaming-distribution*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetStreamingDistributionConfig	授予权限以获取有关串流分配的配置信息	读取	streaming-distribution*		
GetVpcOrigin	授予获取有关 VPC 源信息的权限	读取	vpcorigin*		
ListAnycastIpLists	授予列出你的 Anycast 静态 IP 列表的权限	列表			
ListCachePolicies	授予列出为此账户创建的所有缓存策略 CloudFront 的权限	列表			
ListCloudFrontOriginAccessIdentities	授予列出您的 CloudFront 源站访问身份的权限	列表			
ListConflictingAliases	授予列出与给定别名冲突的所有别名的权限 CloudFront	列表	distribution*		
ListContinuousDeploymentPolicies	授予列出账户中所有持续部署策略的权限	列表			
ListDistributions	授予列出与您关联的分配的权限 Amazon Web Services 账户	列表			
ListDistributionsByAnycastIpListId	授予权限以列出您账户中与指定内容关联的分配 AnycastIp ListId	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListDistributionsByCachePolicyId	IDs 为具有与指定缓存策略关联的缓存行为的分配授予列出分配的权限	列表			
ListDistributionsByKeyGroup	IDs 为具有与指定密钥组关联的缓存行为的分配授予列出分配的权限	列表			
ListDistributionsByLambdaFunction[仅权限]	授予权限以列出与 Lambda 函数关联的分配	列表			
ListDistributionsByOriginRequestPolicyId	IDs 为具有与指定源请求策略关联的缓存行为的分配授予列出分配的权限	列表			
ListDistributionsByRealtimeLogConfig	授予权限以获取具有与指定的实时日志配置关联的缓存行为的分配列表	列表			
ListDistributionsByResponseHeadersPolicyId	IDs 为具有与指定响应标头策略关联的缓存行为的分配授予列出分配的权限	列表			
ListDistributionsByVpcOriginId	授予列 IDs 出与指定 VPC 来源关联的分配的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListDistributionsByWebACLId	授予使用给定 Amazon WAF Web ACL 列出 Amazon Web Services 账户 与您关联的分配的权限	列表			
ListFieldLevelEncryptionConfigs	授予列出为此账户创建的所有字段级加密配置 CloudFront 的权限	列表			
ListFieldLevelEncryptionProfiles	授予列出 CloudFront 为此账户创建的所有字段级加密配置文件的权限	列表			
ListFunctions	授予获取 CloudFront 函数列表的权限	列表			
ListInvalidations	授予权限以列出失效批处理	列表	distribution*		
ListKeyGroups	授予列出为此账户创建的所有密钥组 CloudFront 的权限	列表			
ListKeyValueStores	授予获取以下列表的权限 CloudFront KeyValueStores	列表			
ListOriginAccessControls	授予权限以列出账户中的所有源访问控制	列表			
ListOriginRequestPolicies	授予列出已为此账户创建的所有源请求策略 CloudFront 的权限	列表			
ListPublicKeys	授予列出已为此账户添加的所有公钥 CloudFront 的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListRateCards[仅权限]	授予列出账户 CloudFront 价目表的权限	列表			
ListRealtimeLogConfigs	授予权限以获取实时日志配置列表	列表			
ListResponseHeadersPolicies	授予列出为此账户创建的所有响应标头策略 CloudFront 的权限	列表			
ListSavingsPlans[仅权限]	授予权限以列出账户中的 Savings Plan	列表			
ListStreamingDistributions	授予权限以列出 RTMP 分配	列表			
ListTagsForResource	授予列出 CloudFront 资源标签的权限	读取	anycast-ip-list		
			distribution		
			vpcorigin		
ListUsages[仅权限]	授予列出 CloudFront 使用情况的权限	列表			
ListVpcOrigins	授予列出 VPC 来源的权限	列表			
PublishFunction	授予发布 CloudFront 函数的权限	写入	function*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
TagResource	授予向 CloudFront 资源添加标签的权限	标记	anycast-ip-list		
			distribution		
			streaming-distribution		
			vpcorigin		
				aws:RequestTag/${TagKey} aws:TagKeys	
TestFunction	授予测试 CloudFront 函数的权限	写入	function*		
UntagResource	授予从 CloudFront 资源中移除标签的权限	标记	anycast-ip-list		
			distribution		
			streaming-distribution		
			vpcorigin		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys	
UpdateCachePolicy	授予权限以更新缓存策略	写入	cache-policy*		
UpdateCloudFrontOriginAccessIdentity	授予设置 CloudFront 源访问身份配置的权限	写入	origin-access-identity*		
UpdateContinuousDeploymentPolicy	授予更新持续部署策略的权限	写入	continuous-deployment-policy*		
UpdateDistribution	授予权限以更新 Web 分配的配置	写入	distribution*		
UpdateDistributionWithStagingConfig	授予权限以将暂存 Web 分配的配置复制到其相应的主 Web 分配	写入	distribution*		
UpdateFieldLevelEncryptionConfig	授予权限以更新字段级加密配置	Write			
UpdateFieldLevelEncryptionProfile	授予权限以更新字段级加密配置文件	写入	field-level-encryption-profile*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateFunction	授予更新 CloudFront 函数的权限	写入	function*		
UpdateKeyGroup	授予权限以更新密钥组	写入			
UpdateKeyValueStore	授予更新权限 CloudFront KeyValueStore	写入	key-value-store*		
UpdateOriginAccessControl	授予权限以更新源访问控制	写入	origin-access-control*		
UpdateOriginRequestPolicy	授予权限以更新源请求策略	Write	origin-request-policy*		
UpdatePublicKey	授予权限以更新公有密钥信息	Write			
UpdateRealtimeLogConfig	授予权限以更新实时日志配置	写入	realtime-log-config*		
UpdateResponseHeadersPolicy	授予权限以更新响应标头策略	写入	response-headers-policy*		
UpdateSavingsPlan[仅权限]	授予权限以更新 Savings Plan	写入			
UpdateStreamingDistribution	授予权限以更新 RTMP 分配的配置	写入	streaming-distribution*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateVpcOrigin	授予更新 VPC 来源的权限	写入	vpcorigin*		

Amazon 定义的资源类型 CloudFront

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
distribution	arn:${Partition}:cloudfront::${Account}:distribution/${DistributionId}	aws:ResourceTag/${TagKey}
streaming-distribution	arn:${Partition}:cloudfront::${Account}:streaming-distribution/${DistributionId}	aws:ResourceTag/${TagKey}
origin-access-identity	arn:${Partition}:cloudfront::${Account}:origin-access-identity/${Id}	
field-level-encryption-config	arn:${Partition}:cloudfront::${Account}:field-level-encryption-config/${Id}	
field-level-encryption-profile	arn:${Partition}:cloudfront::${Account}:field-level-encryption-profile/${Id}	
cache-policy	arn:${Partition}:cloudfront::${Account}:cache-policy/${Id}	

资源类型	ARN	条件键
origin-request-policy	arn:${Partition}:cloudfront::${Account}:origin-request-policy/${Id}	
realtime-log-config	arn:${Partition}:cloudfront::${Account}:realtime-log-config/${Name}	
function	arn:${Partition}:cloudfront::${Account}:function/${Name}	
key-value-store	arn:${Partition}:cloudfront::${Account}:key-value-store/${Name}	
response-headers-policy	arn:${Partition}:cloudfront::${Account}:response-headers-policy/${Id}	
origin-access-control	arn:${Partition}:cloudfront::${Account}:origin-access-control/${Id}	
continuous-deployment-policy	arn:${Partition}:cloudfront::${Account}:continuous-deployment-policy/${Id}	
anycast-ip-list	arn:${Partition}:cloudfront::${Account}:anycast-ip-list/${Id}	aws:ResourceTag/${TagKey}
vpcorigin	arn:${Partition}:cloudfront::${Account}:vpcorigin/${Id}	aws:ResourceTag/${TagKey}

Amazon 的条件密钥 CloudFront

Amazon CloudFront 定义了以下条件密钥，这些条件键可用于 IAM 策略的Condition元素中。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对来筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按附加到资源的标签键值对筛选操作	字符串
aws:TagKeys	根据在请求中是否具有标签键来筛选访问	ArrayOfString

Amazon CloudTrail 的操作、资源和条件键

Amazon CloudTrail （服务前缀:`cloudtrail`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon CloudTrail 定义的操作
- Amazon CloudTrail 定义的资源类型
- Amazon CloudTrail 的条件键

Amazon CloudTrail 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，

以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddTags	授予向跟踪、事件数据存储、频道或仪表板添加一个或多个标签的权限，上限为 50	标记	channel		
			dashboard		
			eventdatastore		
			trail		
				aws:RequestTag/${TagKey} aws:TagKeys	
CancelQuery	授予权限以取消正在运行的查询	写入	eventdatastore*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateChannel	授予权限以创建通道	写入	channel*		cloudtrail:AddTags
			eventdatastore*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDashboard	授予创建仪表板的权限	写入	dashboard*		cloudtrail:AddTags cloudtrail:StartDashboardRefresh cloudtrail:StartQuery
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateEventDataStore	授予权限以创建事件数据存储	写入	eventdatastore*		cloudtrail:AddTags iam:CreateServiceLinkedRole iam:GetRole kms:Decrypt kms:GenerateDataKey organizations:ListAWSServiceAccessForOrganization
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateServiceLinkedChannel[仅权限]	授予创建服务相关通道的权限，该通道指定向服务传送日志数据的设置 Amazon	写入	channel*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateTrail	授予权限以创建跟踪，它指定将日志数据传送到 Amazon S3 存储桶的设置	写入	trail*		cloudtrail:AddTags iam:CreateServiceLinkedRole iam:GetRole organizations:ListAWSServiceAccessForOrganization
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	授予权限以删除通道	写入	channel*		
DeleteDashboard	授予权限以删除控制面板	写入	dashboard*		
DeleteEventDataStore	授予权限以删除事件数据存储	写入	eventdatastore*		
DeleteResourcePolicy	授予从提供的资源中删除资源策略的权限	写入	channel		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			dashboard		
			eventdatastore		
DeleteServiceLinkedChannel[仅权限]	授予删除服务相关通道的权限	写入	channel*		
DeleteTrail	授予权限以删除跟踪	写入	trail*		
DeregisterOrganizationDelegatedAdmin	授予将 Organization Amazon s 成员账户注销为委托管理员的权限	写入			organizations:DeregisterDelegatedAdministrator organizations:ListAWSServiceAccessForOrganization
DescribeQuery	授予权限以列出查询的详细信息	读取	eventdatastore*		
DescribeTrails	授予权限以列出与您的账户的当前区域关联的跟踪的设置	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DisableFederation	授予使用 Glue 数据目录禁用事件数据存储数据 Amazon 联合的权限	写入	eventdatastore*		glue:DeleteDatabase glue:DeleteTable glue:PassConnection lakeformation:DeregisterResource lakeformation:RegisterResource

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
EnableFederation	授予使用 Glue 数据目录启用事件数据存储数据 Amazon 联合的权限	写入	eventdatastore*		glue:CreateDatabase glue:CreateTable iam:GetRole iam:PassRole lakeformation:DeregisterResource lakeformation:RegisterResource
GenerateQuery	授予使用 La CloudTrail ke 查询生成器为指定事件数据存储生成查询的权限	写入	eventdatastore*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GenerateQueryResultsSummary [仅权限]	授予使用 CloudTrail 自然语言生成器为指定查询生成结果摘要的权限	读取	eventdatastore*		cloudtrail:GetQueryResults kms:Decrypt kms:GenerateDataKey
GetChannel	授予返回有关特定通道的信息的权限	读取	channel*		
GetDashboard	授予列出仪表板设置的权限	读取	dashboard*		
GetEventDataStore	授予权限以列出事件数据存储的设置	读取	eventdatastore*		
GetEventDataStoreData	授予使用 Glue 数据目录从事件数据存储中 Amazon 获取数据的权限	读取	eventdatastore*		kms:Decrypt kms:GenerateDataKey
GetEventSelectors	授予权限以列出为跟踪配置的事件选择器的设置	读取	trail*		
GetImport	授予返回有关特定导入的信息的权限	读取			
GetInsightSelectors	授予列出为跟踪或事件数据存储配置的 CloudTrail Insights 选择器的权限	读取	eventdatastore		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			trail		
GetQueryResults	授予权限以提取完整查询的结果	读取	eventdatastore*		kms:Decrypt kms:GenerateDataKey
GetResourcePolicy	授予获取附加到提供的资源中资源策略的权限	读取	channel		
			dashboard		
			eventdatastore		
GetServiceLinkedChannel[仅权限]	授予列出服务相关通道设置的权限	读取	channel*		
GetTrail	授予权限以列出跟踪设置	Read	trail*		
GetTrailStatus	授予权限以检索有关指定跟踪的信息的 JSON 格式列表	读取	trail*		
ListChannels	授予列出当前账户中的通道及其来源名称的权限	列表			
ListDashboards	授予列出与您账户当前区域关联的仪表板的权限	列表			
ListEventDataStores	授予权限以列出与您账户的当前区域关联的事件数据存储	列表			
ListImportFailures	授予返回指定导入的失败列表的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListImports	授予返回所有导入信息的权限，或者返回由 ImportStatus 或目的地选择的一组导入信息的权限	列表			
ListPublicKeys	授予权限以列出使用私有密钥对指定时间范围的跟踪摘要文件进行签名的公有密钥	读取			
ListQueries	授予权限以列出与事件数据存储关联的查询	列表	eventdatastore*		
ListServiceLinkedChannels[仅权限]	授予列出与指定账户的当前区域关联的服务相关通道的权限	列表			
ListTags	授予列出当前区域中跟踪、事件数据存储、频道或仪表板标签的权限	读取	channel		
			dashboard		
			eventdatastore		
			trail		
ListTrails	授予权限以列出与您账户的当前区域关联的跟踪	列表			
LookupEvents	授予权限以查找和检索由您账户中创建、更新或删除资源 CloudTrail 所捕获的 API 活动事件的指标数据	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutEventSelectors	授予权限以便为跟踪创建和更新事件选择器	写入	trail*		
PutInsightSelectors	授予为跟踪或事件数据存储创建和更新 CloudTrail Insights 选择器的权限	写入	eventdatastore		
			trail		
PutResourcePolicy	授予将资源策略附加到提供的资源的权限	写入	channel		
			dashboard		
			eventdatastore		
RegisterOrganizationDelegatedAdmin	授予将 Organizat Amazon ions 成员账户注册为委托管理员的权限	写入			iam:CreateServiceLinkedRole iam:GetRole organizations:ListAWSServiceAccessForOrganization organizations:RegisterDelegatedAdministrator

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
RemoveTags	授予从跟踪、事件数据存储、频道或仪表板中移除标签的权限	标记	channel		
			dashboard		
			eventdatastore		
			trail		
				aws:TagKeys	
RestoreEventDataStore	授予权限以恢复事件数据存储	写入	eventdatastore*		
SearchSampleQueries	授予对 La CloudTrail ke 示例查询执行语义搜索的权限	读取			
StartDashboardRefresh	授予在指定仪表板上开始刷新的权限	写入	dashboard*		cloudtrail:StartQuery
StartEventDataStoreIngestion	授予权限以开始在事件数据存储上提取	写入	eventdatastore*		
StartImport	授予开始将记录的跟踪事件从源 S3 桶导入到目标事件数据存储的权限	写入			
StartLogging	授予开始记录 Amazon API 调用和跟踪日志文件传输的权限	写入	trail*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StartQuery	授予权限以启动指定事件数据存储的新查询	写入	eventdatastore*		kms:Decrypt kms:GenerateDataKey
StopEventDataStoreIngestion	授予权限以停止在事件数据存储上提取	写入	eventdatastore*		
StopImport	授予停止指定导入的权限	写入			
StopLogging	授予停止记录 Amazon API 调用和跟踪日志文件传输的权限	写入	trail*		
UpdateChannel	授予权限以更新通道	写入	channel*		
UpdateDashboard	授予权限以更新控制面板	写入	dashboard*		cloudtrail:StartDashboardRefresh cloudtrail:StartQuery

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateEventDataStore	授予权限以更新事件数据存储	写入	eventdatastore*		iam:CreateServiceLinkedRole iam:GetRole kms:Decrypt kms:GenerateDataKey organizations:ListAWSServiceAccessForOrganization
UpdateServiceLinkedChannel[仅权限]	授予更新服务相关通道设置的权限，以便将日志数据传送到服务 Amazon	写入	channel*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateTrail	授予权限以更新指定日志文件传送的设置	写入	trail*		iam:CreateServiceLinkedRole iam:GetRole organizations:ListAWSServiceAccessForOrganization

Amazon CloudTrail 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

> **Note**
>
> 对于控制 CloudTrail 操作访问权限的策略，资源元素始终设置为 “*”。有关在 IAM 策略 ARNs 中使用资源的信息，请参阅Amazon CloudTrail 用户指南中的如何 Amazon CloudTrail 使用 IAM。

资源类型	ARN	条件键
trail	`arn:${Partition}:cloudtrail:${Region}:${Account}:trail/${TrailName}`	aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
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}

Amazon CloudTrail 的条件键

Amazon CloudTrail 定义了可在 IAM 策略Condition元素中使用的以下条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中的标签键值对筛选访问	字符串
aws:ResourceTag/${TagKey}	按附加到资源的标签筛选访问	字符串
aws:TagKeys	按请求中的标签键筛选访问	ArrayOfString

Amazon 的操作、资源和条件密钥 CloudWatch

Amazon CloudWatch （服务前缀:cloudwatch）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon 定义的操作 CloudWatch
- Amazon 定义的资源类型 CloudWatch
- Amazon 的条件密钥 CloudWatch

Amazon 定义的操作 CloudWatch

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchGetServiceLevelIndicatorReport	授予批量获取服务级别指标报告的权限	读取			
BatchGetServiceLevelObjectiveBudgetReport	授予批量检索服务级别目标预算报告的权限	读取	slo*		
CreateServiceLevelObjective	授予创建服务级别目标的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAlarms	授予权限以删除警报的集合	Write	alarm*		
DeleteAnomalyDetector	授予权限以从您的账户中删除指定的异常检测模型	写入			
DeleteDashboards	授予删除您指定的所有 CloudWatch 仪表板的权限	写入	dashboard*		
DeleteInsightRules	授予权限以删除洞察规则的集合	写入	insight-rule*		
DeleteMetricStream	授予删除您指定的 CloudWatch 指标流的权限	写入	metric-stream*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteServiceLevelObjective	授予删除服务级别目标的权限	写入	slo*		
DescribeAlarmHistory	授予权限以检索指定警报的历史记录	Read	alarm*		
DescribeAlarms	授予权限以描述用户的账户当前拥有的所有警报。	Read	alarm*		
DescribeAlarmsForMetric	授予权限以描述在指定的指标上配置且当前由用户的账户拥有的所有警报。	Read			
DescribeAnomalyDetectors	授予权限以列出已在您的账户中创建的异常检测模型	Read			
DescribeInsightRules	授予权限以描述用户账户当前拥有的所有洞察规则	Read			
DisableAlarmActions	授予权限以禁用针对警报集合的操作	Write	alarm*		
DisableInsightRules	授予权限以禁用洞察规则的集合	Write	insight-rule*		
EnableAlarmActions	授予权限以启用针对警报集合的操作	Write	alarm*		
EnableInsightRules	授予权限以启用洞察规则的集合	写入	insight-rule*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
EnableTopologyDiscovery	授予启用 CloudWatch 拓扑发现的权限	写入			
GenerateQuery	授予根据自然语言提示生成 Metrics Insights 或 Logs Insights 查询字符串的权限	读取			
GetDashboard	授予显示您指定的 CloudWatch 仪表板详细信息的权限	读取	dashboard*		
GetInsightRuleReport	授予权限以针对给定洞察规则，返回在一段时间内前 N 个唯一贡献因素的报告	读取	insight-rule*		
GetMetricData	授予检索批量 CloudWatch 指标数据和对检索到的数据执行指标数学运算的权限	读取			
GetMetricStatistics	授予权限以检索指定指标的统计信息	读取			
GetMetricStream	授予返回 CloudWatch 指标流详细信息的权限	读取	metric-stream*		
GetMetricWidgetImage	授予权限以检索指标小部件的快照	读取			
GetService	授予检索服务相关信息的权限	读取	service*		
GetServiceData[仅权限]	授予检索服务数据的权限	读取	service*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetServiceLevelObjective	授予检索服务级别目标信息的权限	读取	slo*		
GetTopologyDiscoveryStatus[仅权限]	授予检索 CloudWatch 拓扑发现状态的权限	读取			
GetTopologyMap	授予检索 CloudWatch 拓扑图的权限	读取			
Link[仅权限]	授予与监控账户共享 CloudWatch 资源的权限	写入			
ListDashboards	授予返回您账户中所有 CloudWatch 仪表板列表的权限	列表			
ListEntitiesForMetric[仅权限]	授予权限以检索发出给定指标的所有实体	列表			
ListManagedInsightRules	授予列出给定资源 ARN 的可用托管式洞察规则的权限	读取		aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:requestManagedResourceARNs	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListMetricStreams	授予返回您账户中所有 CloudWatch 指标流列表的权限	列表			
ListMetrics	授予权限以检索为 Amazon Web Services 账户 所有者存储的有效指标列表	列表			
ListServiceLevelObjectives	授予列出服务级别目标的权限	列表			
ListServices	授予列出服务的权限	列表			
ListTagsForResource	授予列出 Amazon CloudWatch 资源标签的权限	列表	alarm		
			insight-rule		
			slo		
	场景：CloudWatch-Alarm		alarm*		
	场景：CloudWatch-Insight Rule		insight-rule*		
	场景：CloudWatch-Service LevelObjective		slo*		
PutAnomalyDetector	授予为指标创建或更新异常检测模型的 CloudWatch 权限	写入			
PutCompositeAlarm	授予权限以创建或更新复合警报	写入	alarm*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:AlarmActions	
PutDashboard	授予创建 CloudWatch 仪表板或更新现有仪表板（如果已存在）的权限	写入	dashboard*		
PutInsightRule	授予权限以创建新洞察规则或替换现有洞察规则	写入	insight-rule*		
				aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:requestInsightRuleLogGroups	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutManagedInsightRules	授予创建托管式洞察规则的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:requestManagedResourceARNs	
PutMetricAlarm	授予创建或更新警报并将其与指定的 Amazon CloudWatch 指标关联的权限	写入	alarm*		
				aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:AlarmActions	
PutMetricData	授予向 Amazon 发布指标数据点的权限 CloudWatch	写入		cloudwatch:namespace	
PutMetricStream	授予创建 CloudWatch 指标流或更新现有指标流（如果已存在）的权限	写入	metric-stream*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
SetAlarmState	授予权限以出于测试目的临时设置警报的状态	写入	alarm*		
StartMetricStreams	授予启动您指定的所有 CloudWatch 指标流的权限	写入	metric-stream*		
StopMetricStreams	授予停止您指定的所有 CloudWatch 指标流的权限	写入	metric-stream*		
TagResource	授予向 Amazon CloudWatch 资源添加标签的权限	标记	alarm		
			insight-rule		
			slo		
				aws:TagKeys aws:RequestTag/${TagKey}	
	场景：CloudWatch-Alarm		alarm*		
	场景：CloudWatch-Insight Rule		insight-rule*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
	场景：CloudWatch-ServiceLevelObjective		slo*		
UntagResource	授予从 Amazon CloudWatch 资源中移除标签的权限	标记	alarm		
			insight-rule		
			slo		
				aws:TagKeys	
	场景：CloudWatch-Alarm		alarm*		
	场景：CloudWatch-Insight Rule		insight-rule*		
	场景：CloudWatch-ServiceLevelObjective		slo*		
UpdateServiceLevelObjective	授予更新服务级别目标的权限	写入	slo*		

Amazon 定义的资源类型 CloudWatch

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
alarm	arn:${Partition}:cloudwatch:${Region}:${Account}:alarm:${AlarmName}	aws:ResourceTag/${TagKey}
dashboard	arn:${Partition}:cloudwatch::${Account}:dashboard/${DashboardName}	
insight-rule	arn:${Partition}:cloudwatch:${Region}:${Account}:insight-rule/${InsightRuleName}	aws:ResourceTag/${TagKey}
metric-stream	arn:${Partition}:cloudwatch:${Region}:${Account}:metric-stream/${MetricStreamName}	aws:ResourceTag/${TagKey}
slo	arn:${Partition}:cloudwatch:${Region}:${Account}:slo/${SloName}	aws:ResourceTag/${TagKey}
service	arn:${Partition}:cloudwatch:${Region}:${Account}:service/${ServiceName}-${UniqueAttributesHex}	aws:ResourceTag/${TagKey}

Amazon 的条件密钥 CloudWatch

Amazon CloudWatch 定义了以下条件密钥，这些条件键可用于 IAM 策略的Condition元素中。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据每个标签的允许值集筛选操作	字符串
aws:ResourceTag/${TagKey}	根据与资源关联的标签值筛选操作	字符串

条件键	描述	类型
aws:TagKeys	根据在请求中是否具有必需标签以筛选操作	ArrayOfString
cloudwatch:AlarmActions	根据定义的警报操作筛选操作	ArrayOfString
cloudwatch:namespace	根据是否存在可选命名空间值来筛选操作	字符串
cloudwatch:requestInsightRuleLogGroups	根据 Insight 规则中指定的日志组筛选操作	ArrayOfString
cloudwatch:requestManagedResourceARNs	按托管智能分析规则中 ARNs 指定的资源筛选访问权限	ArrayOfARN

Amazon App CloudWatch lication Insights 的操作、资源和条件键

Amazon App CloudWatch lication Insights（服务前缀:`applicationinsights`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- 由 Amazon CloudWatch 应用程序见解定义的操作
- 由 Amazon CloudWatch 应用程序见解定义的资源类型
- Amazon CloudWatch 应用程序见解的条件密钥

由 Amazon CloudWatch 应用程序见解定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddWorkload	授予添加工作负载的权限	写入			
CreateApplication	授予从资源组创建应用程序的权限	Write			
CreateComponent	授予从一组资源创建组件的权限	Write			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateLogPattern	授予创建日志模式的权限	Write			
DeleteApplication	授予删除应用程序的权限	Write			
DeleteComponent	授予删除组件的权限	Write			
DeleteLogPattern	授予删除日志模式的权限	Write			
DescribeApplication	授予描述应用程序的权限	Read			
DescribeComponent	授予描述组件的权限	Read			
DescribeComponentConfiguration	授予描述组件配置的权限	Read			
DescribeComponentConfigurationRecommendation	授予描述推荐的应用程序组件配置的权限	Read			
DescribeLogPattern	授予描述日志模式的权限	Read			
DescribeObservation	授予描述观察的权限	Read			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeProblem	授予描述问题的权限	Read			
DescribeProblemObservations	授予描述问题中观察的权限	读取			
DescribeWorkload	授予描述工作负载的权限	读取			
Link[仅权限]	授予与监控账户共享 Application Insights 资源的权限	写入			
ListApplications	授予列出所有应用程序的权限	List			
ListComponents	授予列出应用程序组件的权限	List			
ListConfigurationHistory	授予列出配置历史记录的权限	List			
ListLogPatternSets	授予列出应用程序的日志模式集的权限	List			
ListLogPatterns	授予列出日志模式的权限	List			
ListProblems	授予列出应用程序中问题的权限	List			
ListTagsForResource	授予列出资源标签的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListWorkloads	授予列出工作负载的权限	列表			
RemoveWorkload	授予移除工作负载的权限	写入			
TagResource	授予权限以标记资源	Tagging		aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予权限以取消标记资源	Tagging		aws:TagKeys	
UpdateApplication	授予更新应用程序的权限	Write			
UpdateComponent	授予更新组件的权限	Write			
UpdateComponentConfiguration	授予更新组件配置的权限	Write			
UpdateLogPattern	授予更新日志模式的权限	写入			
UpdateProblem	授予更新问题的权限	写入			
UpdateWorkload	授予更新工作负载的权限	写入			

由 Amazon CloudWatch 应用程序见解定义的资源类型

Amazon App CloudWatch lication Insights 不支持在 IAM 政策声明的`Resource`元素中指定资源 ARN。要允许访问 Amazon App CloudWatch lication Insights，请在您的政策`"Resource": "*"`中指定。

Amazon CloudWatch 应用程序见解的条件密钥

Amazon App CloudWatch lication Insights 定义了以下可用于 IAM 策略`Condition`元素的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中允许的标签键值对筛选访问	字符串
aws:ResourceTag/${TagKey}	按某个资源的标签键值对筛选访问	字符串
aws:TagKeys	按请求中允许的标签键列表筛选访问	ArrayOfString

Amazon CloudWatch 日志的操作、资源和条件密钥

Ama CloudWatch zon Logs（服务前缀:`logs`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- 由 Amazon CloudWatch 日志定义的操作
- 由 Amazon CloudWatch 日志定义的资源类型

- Amazon CloudWatch 日志的条件密钥

由 Amazon CloudWatch 日志定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateKmsKey	授予将指定的 Amazon 密钥管理服务 (Amazon KMS) 客户主密钥 (CMK) 与指定日志组关联的权限	写入	log-group *		
CancelExportTask	授予权限，如果导出任务处于 PENDING（待处理）或	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
	RUNNING（正在运行）状态，则取消该任务				
CreateDelivery	授予创建将传输源连接到传输目标的传输的权限	写入	delivery*		
			delivery-destination*		
			delivery-source*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateExportTask	授予创建权限 ExportTask ，允许您高效地将数据从日志组导出到 Amazon S3 存储桶	写入	log-group*		
CreateLogAnomalyDetector	授予创建日志异常检测器的权限	写入	log-group*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateLogDelivery[仅权限]	授予权限以创建日志传送	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateLogGroup	授予权限以创建具有指定名称的新日志组	写入	log-group*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateLogStream	授予权限以创建具有指定名称的新日志流	写入	log-stream*		
DeleteAccountPolicy	授予删除账户策略的权限	写入			
DeleteDataProtectionPolicy	授予权限以删除附加到日志组的数据保护策略	写入	log-group*		
DeleteDelivery	授予删除传输的权限	写入	delivery*		
DeleteDeliveryDestination	授予删除所有关联的传输后删除传输目标的权限	写入	delivery-destination*		
DeleteDeliveryDestinationPolicy	授予删除与传输目标关联的传输目标策略的权限	写入	delivery-destination*		
DeleteDeliverySource	授予删除所有关联的传输后删除传输源的权限	写入	delivery-destination*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteDestination	授予权限以删除具有指定名称的目标	写入	destination*		
DeleteIndexPolicy	授予删除附加到日志组的索引策略的权限	写入			
DeleteIntegration	授予删除集成的权限	写入			
DeleteLogAnomalyDetector	授予删除日志异常探测器的权限	写入	anomaly-detector*		
DeleteLogDelivery[仅权限]	授予权限以删除指定日志传送的日志传送信息	写入			
DeleteLogGroup	授予权限以删除具有指定名称的日志组	写入	log-group*		
DeleteLogStream	授予权限以删除日志流	写入	log-stream*		
DeleteMetricFilter	授予权限以删除与指定日志组关联的指标筛选条件	写入	log-group*		
DeleteQueryDefinition	授予删除已保存的 L CloudWatch ogs Insights 查询定义的权限	写入			
DeleteResourcePolicy	授予权限以从此账户删除资源策略	权限管理			
DeleteRetentionPolicy	授予权限以删除指定日志组的保留策略	写入	log-group*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteSubscriptionFilter	授予权限以删除与指定日志组关联的订阅筛选条件	写入	log-group *		
DeleteTransformer	授予删除与指定日志组关联的转换器的权限	写入	log-group *		
DescribeAccountPolicies	授予检索账户政策的权限	列表			
DescribeConfigurationTemplates	授予权限以检索可用日志类型的配置模板列表	列表			
DescribeDeliveries	授予检索账户中的传输列表的权限	列表			
DescribeDeliveryDestinations	授予检索账户中的传输目标列表的权限	列表			
DescribeDeliverySources	授予检索账户中的传输源列表的权限	列表			
DescribeDestinations	授予返回与提出请求相关的所有目的地的权限 Amazon Web Services 账户	列表			
DescribeExportTasks	授予返回与提出请求相关的所有导出任务的权限 Amazon Web Services 账户	列表			
DescribeFieldIndexes	授予返回与日志组关联的所有索引属性的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeIndexPolicies	授予返回与日志组关联的所有索引策略的权限	列表			
DescribeLogGroups	授予返回与发出请求关联的所有日志组的权限 Amazon Web Services 账户	列表			
DescribeLogStreams	授予权限以返回与指定日志组关联的所有日志流	列表	log-group *		
DescribeMetricFilters	授予权限以返回与指定日志组关联的所有指标筛选条件	列表	log-group *		
DescribeQueries	授予返回此账户中已计划、正在执行或最近执行的 L CloudWatch ogs Insights 查询列表的权限	列表			
DescribeQueryDefinitions	授予返回已保存的 Lo CloudWatch gs Insights 查询定义的分页列表的权限	列表			
DescribeResourcePolicies	授予权限以返回此账户中的所有资源策略	列表			
DescribeSubscriptionFilters	授予权限以返回与指定日志组关联的所有订阅筛选条件	列表	log-group *		
DisassociateKmsKey	授予权限以解除关联的 Amazon 密钥管理服务 (Amazon KMS) 客户主密钥 (CMK) 与指定日志组的关联	写入	log-group *		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
FilterLogEvents	授予权限以从指定日志组中检索日志事件，可以选择通过筛选条件模式进行筛选	读取	log-group*		
GetDataProtectionPolicy	授予权限以检索附加到日志组的数据保护策略	读取	log-group*		
GetDelivery	授予检索单个传输的权限	读取	delivery*		
GetDeliveryDestination	授予检索单个传输目标的权限	读取	delivery-destination*		
GetDeliveryDestinationPolicy	授予检索附加到传输目标的传输目标策略的权限	读取	delivery-destination*		
GetDeliverySource	授予检索单个传输源的权限	读取	delivery-source*		
GetIntegration	授予检索单个集成的权限	读取			
GetLogAnomalyDetector	授予获取日志异常检测器的权限	读取	anomaly-detector*		
GetLogDelivery[仅权限]	授予权限以获取指定日志传送的日志传送信息	读取			
GetLogEvents	授予权限以从指定日志流中检索日志事件	读取	log-stream*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetLogGroupFields	授予权限以返回指定日志组中的日志事件包含的字段列表，以及包含每个字段的日志事件的百分比	读取	log-group *		
GetLogRecord	授予权限以检索单个日志事件的所有字段和值	读取	log-group *		
GetQueryResults	授予权限以返回指定查询的结果	读取	log-group *		
GetTransformer	授予返回与指定日志组关联的转换器的权限	读取	log-group *		
Link[仅权限]	授予与监控账户共享 CloudWatch 资源的权限	写入			
ListAnomalies	授予列出在 Amazon Web Services 账户 提出请求时检测到的所有异常的权限	列表	anomaly-detector		
ListEntitiesForLogGroup[仅权限]	授予检索与日志组关联的所有实体的权限	列表			
ListIntegrations	授予列出与 Amazon Web Services 账户 提出请求相关的所有集成的权限	列表			
ListLogAnomalyDetectors	授予返回与 Amazon Web Services 账户 发出请求关联的所有异常检测器的权限	列表	anomaly-detector		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListLogDeliveries[仅权限]	授予权限以列出指定账户和/或日志源的所有日志传送	列表			
ListLogGroupsForEntity[仅权限]	授予检索与实体关联的所有日志组的权限	列表			
ListLogGroupsForQuery	授予返回与指定查询关联的所有日志组的权限	列表			
ListTagsForResource	授予权限以列出指定资源的标签	列表	anomaly-detector		
			delivery		
			delivery-destination		
			delivery-source		
			destination		
			log-group		
ListTagsLogGroup	授予权限以列出指定日志组的标签	列表	log-group *		
PutAccountPolicy	授予附加账户政策的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutDataProtectionPolicy	授予权限以附加数据保护策略，以检测和编辑日志事件中的敏感信息	写入	log-group*		
PutDeliveryDestination	授予创建/更新传输目标的权限	写入	delivery-destination*		
				aws:TagKeys aws:RequestTag/${TagKey} logs:DeliveryDestinationResourceArn	
PutDeliveryDestinationPolicy	授予将传输目标策略附加到传输目标的权限	写入	delivery-destination*		
PutDeliverySource	授予创建/更新传输源的权限	写入	delivery-source*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys aws:RequestTag/${TagKey} logs:LogGeneratingResourceArns	
PutDestination	授予权限以创建或更新目标	写入	destination*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey}	
PutDestinationPolicy	授予权限以创建或更新与现有目标关联的访问策略	写入	destination*		
PutIndexPolicy	授予在日志组级别附加索引策略以优化搜索和查询的权限	写入			
PutIntegration	授予在 cloudwatch 日志和开放搜索之间创建集成的权限	写入			
PutLogEvents	授予权限以将一批日志事件上传到指定的日志流	写入	log-stream*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutMetricFilter	授予权限以创建或更新指标筛选条件并将其与指定日志组关联	写入	log-group *		
PutQueryDefinition	授予权限以创建或更新查询定义	写入			
PutResourcePolicy	授予创建或更新资源策略的权限，允许其他 Amazon 服务将日志事件存入此账户	权限管理			
PutRetentionPolicy	授予权限以设置指定日志组的保留	写入	log-group *		
PutSubscriptionFilter	授予权限以创建或更新订阅筛选器并将其与指定日志组关联	写入	log-group *		iam:PassRole
			destination		
PutTransformer	授予创建或更新转换器并将其与指定日志组关联的权限	写入	log-group *		
StartLiveTail	授予在 CloudWatch 日志中启动 Live Tail 会话的权限	读取	log-group *		
StartQuery	授予使用 Logs Insights 计划对日志组进行 CloudWatch 查询的权限	读取	log-group *		
StopLiveTail[仅权限]	授予停止正在执行的 Live Tail 会话的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StopQuery	授予停止正在进行的 CloudWatch Logs Insights 查询的权限	读取			
TagLogGroup	授予权限以为指定日志组添加或更新指定的标签	标记	log-group *		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagResource	授予权限以将指定标签添加到指定资源或进行更新	标记	anomaly-detector		
			delivery		
			delivery-destination		
			delivery-source		
			destination		
			log-group		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys aws:RequestTag/${TagKey}	
TestMetricFilter	授予权限以针对日志事件消息示例测试指标筛选条件的筛选条件模式	读取			
TestTransformer	授予根据日志事件消息样本测试转换器的权限	读取			
Unmask[仅权限]	授予权限以获取已通过数据保护策略编辑的未屏蔽日志事件	读取	log-group *		
UntagLogGroup	授予权限以删除指定日志组的指定标签	标记	log-group *		
				aws:TagKeys	
UntagResource	授予权限以从指定资源中删除指定标签	标记	anomaly-detector		
			delivery		
			delivery-destination		
			delivery-source		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			destination		
			log-group		
				aws:TagKeys	
UpdateAnomaly	授予更新日志异常检测器所报告异常的权限	写入	anomaly-detector*		
UpdateDeliveryConfiguration	授予权限以更新与交付相关的配置	写入	delivery*		
			delivery-destination*		
			delivery-source*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateLogAnomalyDetector	授予更新日志异常检测器的权限	写入	anomaly-detector*		
UpdateLogDelivery[仅权限]	授予权限以更新指定日志传送的日志传送信息	写入			

由 Amazon CloudWatch 日志定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
log-group	arn:${Partition}:logs:${Region}:${Account}:log-group:${LogGroupName}	aws:ResourceTag/${TagKey}
log-stream	arn:${Partition}:logs:${Region}:${Account}:log-group:${LogGroupName}:log-stream:${LogStreamName}	aws:ResourceTag/${TagKey}
destination	arn:${Partition}:logs:${Region}:${Account}:destination:${DestinationName}	aws:ResourceTag/${TagKey}
delivery-source	arn:${Partition}:logs:${Region}:${Account}:delivery-source:${DeliverySourceName}	aws:ResourceTag/${TagKey}
delivery	arn:${Partition}:logs:${Region}:${Account}:delivery:${DeliveryName}	aws:ResourceTag/${TagKey}
delivery-destination	arn:${Partition}:logs:${Region}:${Account}:delivery-destination:${DeliveryDestinationName}	aws:ResourceTag/${TagKey}
anomaly-detector	arn:${Partition}:logs:${Region}:${Account}:anomaly-detector:${DetectorId}	aws:ResourceTag/${TagKey}

Amazon CloudWatch 日志的条件密钥

A CloudWatch mazon Logs 定义了以下可在 IAM 策略Condition元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString
logs:DeliveryDestinationResourceArn	按请求中传递的日志目标 ARN 筛选访问权限	ARN
logs:LogGenerating ResourceArns	按请求中 ARNs 传递的日志生成资源筛选访问权限	ArrayOfARN

Amazon CloudWatch 可观察性访问管理器的操作、资源和条件密钥

Amazon O CloudWatch bservability Access Manager（服务前缀:oam）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon CloudWatch 可观察性访问管理器定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateLink	授予权限以在监控账户和源账户之间创建链接，以进行跨账户监控	写入	Sink*		oam:TagResource

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys oam:ResourceTypes	
CreateSink	授予权限以在账户中创建接收器，以便该账户可用作跨账户监控的监控账户	写入		aws:RequestTag/${TagKey} aws:TagKeys	oam:TagResource
DeleteLink	授予权限以在监控账户和源账户之间删除链接，以进行跨账户监控	写入	Link*		
				aws:ResourceTag/${TagKey}	
DeleteSink	授予权限以删除监控账户中跨账户监控接收器	写入	Sink*		
				aws:ResourceTag/${TagKey}	
GetLink	授予权限以检索有关一个跨账户监控链接的完整信息	读取	Link*		
				aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetSink	授予权限以检索有关一个跨账户监控接收器的完整信息	读取	Sink*		
				aws:ResourceTag/${TagKey}	
GetSinkPolicy	授予权限以检索跨账户监控接收器的 IAM policy 的信息	读取	Sink*		
				aws:ResourceTag/${TagKey}	
ListAttachedLinks	授予权限以检索为跨账户监控接收器链接的链接列表	读取	Sink*		
				aws:ResourceTag/${TagKey}	
ListLinks	授予检索此账户 ARNs 中跨账户监控链接的权限	读取			
ListSinks	授予检索此账户 ARNs 中跨账户监控接收器的权限	读取			
ListTagsForResource	授予列出资源标签的权限	读取	Link		
			Sink		
PutSinkPolicy	授予权限以创建或更新跨账户监控接收器的 IAM policy	写入	Sink*		
				aws:ResourceTag/${TagKey}	
TagResource	授予权限以标记资源	Tagging	Link		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			Sink		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予权限以取消标记资源	标记	Link		
			Sink		
				aws:TagKeys	
UpdateLink	授予权限以更新监控账户和源账户之间的现有链接	写入	Link*		
				aws:ResourceTag/${TagKey} oam:ResourceTypes	

由 Amazon CloudWatch 可观察性访问管理器定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
Link	arn:${Partition}:oam:${Region}:${Account}:link/${ResourceId}	aws:ResourceTag/${TagKey}
Sink	arn:${Partition}:oam:${Region}:${Account}:sink/${ResourceId}	aws:ResourceTag/${TagKey}

Amazon CloudWatch 可观察性访问管理器的条件密钥

Amazon O CloudWatch bservability Access Manager 定义了以下可用于 IAM 策略Condition元素的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对来筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按附加到资源的标签键值对筛选操作	字符串
aws:TagKeys	根据在请求中是否具有标签键来筛选访问	ArrayOfString
oam:ResourceTypes	按请求中的资源类型筛选访问权限	ArrayOfString

Amazon Sy CloudWatch nthetics 的操作、资源和条件密钥

Ama CloudWatch zon Synthetics（服务前缀:synthetics）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。

- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- 由 Amazon S CloudWatch ynthetics 定义的操作
- 由 Amazon S CloudWatch ynthetics 定义的资源类型
- Amazon Sy CloudWatch nthetics 的条件密钥

由 Amazon S CloudWatch ynthetics 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateResource	授予权限以将资源与组相关联	写入	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
CreateCanary	授予权限以创建 Canary	写入		aws:RequestTag/${TagKey} aws:TagKeys	
CreateGroup	授予权限以创建组	写入		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCanary	授予权限以删除 Canary。Amazon Synthetics 会删除除 Lambda 函数和警报（如果您创建了 CloudWatch 警报）之外的所有资源	写入	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteGroup	授予权限以删除组	写入	group*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} aws:TagKeys	
DescribeCanaries	授予权限以列出所有 Canary 信息	Read		synthetics:Names	
DescribeCanariesLastRun	授予权限以列出有关与所有 Canary 关联的最后一次测试运行的信息	Read		synthetics:Names	
DescribeRuntimeVersions	授予列出有关 Synthetics Canary 运行时版本信息的权限	读取			
DisassociateResource	授予权限以取消资源与组的关联	写入	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
GetCanary	授予权限以查看 Canary 详细信息	读取	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetCanaryRuns	授予权限以列出有关所有与 Canary 关联的测试运行的信息	读取	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
GetGroup	授予权限以查看组详细信息	读取	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ListAssociatedGroups	授予权限以列出有关 Canary 关联组的信息	列表	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ListGroupResources	授予权限以列出有关组中的 Canary 的信息	列表	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListGroups	授予权限以列出所有组的信息	列表			
ListTagsForResource	授予权限以列出与资源关联的所有标签和值	读取	canary		
			group		
StartCanary	授予启动金丝雀的权限，以便 Amazon Sy CloudWatch nthetics 开始监控网站	写入	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
StopCanary	授予权限以停止 Canary	写入	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
TagResource	授予权限以将一个或多个标签添加到资源中	Tagging	canary		
			group		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UntagResource	授予从资源删除一个或多个标签的权限	标记	canary		
			group		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCanary	授予权限以更新 Canary	写入	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

由 Amazon S CloudWatch ynthetics 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
canary	arn:${Partition}:synthetics:${Region}:${Account}:canary:${CanaryName}	aws:ResourceTag/${TagKey}
group	arn:${Partition}:synthetics:${Region}:${Account}:group:${GroupId}	aws:ResourceTag/${TagKey}

Amazon Sy CloudWatch nthetics 的条件密钥

Ama CloudWatch zon Synthetics 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中传递的标签筛选访问	字符串
aws:ResourceTag/${TagKey}	根据与资源关联的标签筛选访问	字符串
aws:TagKeys	根据在请求中传递的标签键筛选访问	ArrayOfString
synthetics:Names	根据 Canary 的名称筛选访问权限	ArrayOfString

Amazon CodeBuild 的操作、资源和条件键

Amazon CodeBuild （服务前缀:codebuild）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon CodeBuild 定义的操作
- Amazon CodeBuild 定义的资源类型
- Amazon CodeBuild 的条件键

Amazon CodeBuild 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchDeleteBuilds	授予权限以删除一个或多个构建	写入	project*		
BatchGetBuildBatches	授予权限以获取一个或多个构建批处理的相关信息	读取	project*		
BatchGetBuilds	授予权限以获取一个或多个构建的相关信息	读取	project*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchGetFleets	授予权限以返回由输入参数指定的 Fleet 对象的数组	读取	fleet*		
BatchGetProjects	授予权限以获取一个或多个构建项目的相关信息	读取	project*		
BatchGetReportGroups	授予返回由输入 reportGroupArns 参数指定的 ReportGroup 对象数组的权限	读取	report-group*		
BatchGetReports	授予权限以返回由输入 reportArns 参数指定的 Report 对象的数组	读取	report-group*		
BatchPutCodeCoverages[仅权限]	授予权限以添加或更新有关报告的信息	写入	report-group*		
BatchPutTestCases[仅权限]	授予权限以添加或更新有关报告的信息	写入	report-group*		
CreateFleet	授予权限以创建计算实例集	写入	fleet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProject	授予权限以创建构建项目	写入	project*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateReport[仅权限]	授予权限以创建报告。当 buildspec 文件中为报告组指定的测试在项目构建期间运行时，将创建报告	写入	report-group*		
CreateReportGroup	授予权限以创建报告组	写入	report-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebhook	授予权限以创建 Webhook。对于源代码存储在 GitHub 或 Bitbucket 存储库中的现有 Amazon CodeBuild 构建项目，Amazon CodeBuild 允许在每次将代码更改推送到存储库时开始重建源代码	写入	project*		
DeleteBuildBatch	授予权限以删除构建批处理	写入	project*		
DeleteFleet	授予权限以删除计算实例集	写入	fleet*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteOAuthToken[仅权限]	授予从关联的第三方 OAuth 提供商删除 OAuth 令牌的权限。仅在 Amazon CodeBuild 控制台中使用	写入			
DeleteProject	授予权限以删除构建项目	写入	project*		
DeleteReport	授予权限以删除报告	写入	report-group*		
DeleteReportGroup	授予权限以删除报告组	写入	report-group*		
DeleteResourcePolicy	授予权限以删除关联的项目或报告组的资源策略	权限管理	project report-group		
DeleteSourceCredentials	授予删除一组 GitHub、GitHub 企业版或 Bitbucket 源凭证的权限	写入			
DeleteWebhook	授予权限以删除 Webhook。对于源代码存储在 GitHub 或 Bitbucket 存储库中的现有 Amazon CodeBuild 构建项目，每次将代码更改推送 Amazon CodeBuild 到存储库时都停止重建源代码	写入	project*		
DescribeCodeCoverages	授予返回 CodeCoverage 对象数组的权限	读取	report-group*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeTestCases	授予返回 TestCase 对象数组的权限	读取	report-group*		
GetReportGroupTrend	授予权限以分析和累积指定报告组中测试报告的测试报告值	读取	report-group*		
GetResourcePolicy	授予权限以返回指定项目或报告组的资源策略	读取	project		
			report-group		
ImportSourceCredentials	授予导入源代码存储在 GitHub、E GitHub nterprise 或 Bitbucket 存储库中的 Amazon CodeBuild 项目的源存储库凭据的权限	写入			
InvalidateProjectCache	授予权限以重置项目缓存	写入	project*		
ListBuildBatches	授予获取生成批次列表的权限 IDs，每个生成批次 ID 代表一个构建批次	列表			
ListBuildBatchesForProject	授予获取指定构建项目的生成批次列表 IDs 的权限，每个生成批次 ID 代表一个生成批次	列表	project*		
ListBuilds	授予获取版本列表的权限 IDs，每个构建 ID 代表一个构建	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListBuildsForProject	授予获取指定构建项目的版本列表 IDs 的权限，每个构建 ID 代表一个构建	列表	project*		
ListConnectedOAuthAccounts[仅权限]	授予列出关联第三方 OAuth 提供商的权限。仅在 Amazon CodeBuild 控制台中使用	列表			
ListCuratedEnvironmentImages	授予权限以获取有关由管理的 Docker 镜像的信息 Amazon CodeBuild	列表			
ListFleets	授予获取计算队列列表的权限 ARNs，每个计算队列 ARN 代表一个队列	列表			
ListProjects	授予权限以获取构建项目名称的列表，其中每个构建项目名称代表一个构建项目	列表			
ListReportGroups	授予返回报告组列表的权限 ARNs。每个报告组 ARN 代表一个报告组	列表			
ListReports	授予返回报告列表的权限 ARNs。每个报告 ARN 表示一个报告	列表			
ListReportsForReportGroup	授予返回 ARNs 属于指定报告组的报告列表的权限。每个报告 ARN 表示一个报告	列表	report-group*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListRepositories[仅权限]	授予列出来自关联第三方 OAuth 提供商的源代码存储库的权限。仅在 Amazon CodeBuild 控制台中使用	列表			
ListSharedProjects	授予返回已与请求者共享 ARNs 的项目列表的权限。每个项目 ARN 表示一个项目	列表			
ListSharedReportGroups	授予返回已与请求者共享的报告组 ARNs 列表的权限。每个报告组 ARN 代表一个报告组	列表			
ListSourceCredentials	授予返回 SourceCredentialsInfo 对象列表的权限	列表			
PersistOAuthToken[仅权限]	授予保存来自关联第三方 OAuth 提供商的 OAuth 令牌的权限。仅在 Amazon CodeBuild 控制台中使用	写入			
PutResourcePolicy	授予权限以为关联的项目或报告组创建资源策略	权限管理	project		
			report-group		
RetryBuild	授予权限以重试构建	写入	project*		
RetryBuildBatch	授予权限以重试构建批处理	写入	project*		
StartBuild	授予权限以开始运行构建	写入	project*		
StartBuildBatch	授予权限以开始运行构建批处理	写入	project*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StopBuild	授予权限以尝试停止运行构建	写入	project*		
StopBuildBatch	授予权限以尝试停止运行构建批处理	写入	project*		
UpdateFleet	授予权限以更改现有计算实例集的设置	写入	fleet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateProject	授予权限以更改现有构建项目的设置	写入	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateProjectVisibility	授予权限以更改项目及其构建的公共可见性	写入	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateReport[仅权限]	授予权限以更新有关报告的信息	写入	report-group*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateReportGroup	授予权限以更改现有报告组的设置	写入	report-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateWebhook	授予更新与 Amazon CodeBuild 构建项目关联的 webhook 的权限	写入	project*		

Amazon CodeBuild 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
build	arn:${Partition}:codebuild:${Region}:${Account}:build/${BuildId}	
build-batch	arn:${Partition}:codebuild:${Region}:${Account}:build-batch/${BuildBatchId}	
project	arn:${Partition}:codebuild:${Region}:${Account}:project/${ProjectName}	aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
report-group	arn:${Partition}:codebuild:${Region}:${Account}:report-group/${ReportGroupName}	aws:ResourceTag/${TagKey}
report	arn:${Partition}:codebuild:${Region}:${Account}:report/${ReportGroupName}:${ReportId}	
fleet	arn:${Partition}:codebuild:${Region}:${Account}:fleet/${FleetName}:${FleetId}	

Amazon CodeBuild 的条件键

Amazon CodeBuild 定义了可在 IAM 策略Condition元素中使用的以下条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对来按照操作筛选访问权限	字符串
aws:ResourceTag/${TagKey}	根据附加到资源的标签键值对来按操作筛选访问权限	字符串
aws:TagKeys	根据在请求中是否具有标签键来按操作筛选访问权限	ArrayOfString
codebuild:buildArn	按发起请求的 Amazon CodeBuild 版本的 ARN 筛选访问权限	ARN
codebuild:projectArn	按发起请求的 Amazon CodeBuild 项目的 ARN 筛选访问权限	ARN

Amazon CodeCommit 的操作、资源和条件键

Amazon CodeCommit （服务前缀:codecommit）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon CodeCommit 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateApprovalRuleTemplateWithRepository	授予权限以将批准规则模板与存储库关联	Write	repository*		
BatchAssociateApprovalRuleTemplateWithRepositories	授予权限以在单个操作中将一个批准规则模板与多个存储库关联	Write	repository*		
BatchDescribeMergeConflicts	授予权限以获取有关在尝试使用三向合并或压缩合并选项合并两个提交时发生的多个合并冲突的信息	Read	repository*		
BatchDisassociateApprovalRuleTemplateFromRepositories	授予权限以在单个操作中删除一个批准规则模板与多个存储库之间的关联	写入	repository*		
BatchGetCommits	授予返回 Amazon CodeCommit 仓库中一个或多个提交信息的权限	读取	repository*		
BatchGetPullRequests[仅权限]	授予返回 Amazon CodeCommit 仓库中一个或多个拉取请求信息的权限	读取	repository*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchGetRepositories	授予权限以获取有关多个存储库的信息	Read	repository*		
CancelUploadArchive[仅权限]	授予取消将档案上传到管道的权限 Amazon CodePipeline	读取	repository*		
CreateApprovalRuleTemplate	授予权限以创建批准规则模板，该模板将在拉取请求中自动创建与模板中定义的条件匹配的批准规则；不授予为单个拉取请求创建批准规则的权限	写入			
CreateBranch	授予使用此 API 在 Amazon CodeCommit 仓库中创建分支的权限；不控制 Git 创建分支操作	写入	repository*		
				codecommit:References	
CreateCommit	授予添加、复制、移动或更新 Amazon CodeCommit 存储库中分支中的单个或多个文件的权限，以及为指定分支中的更改生成提交信息的权限	写入	repository*		
				codecommit:References	
CreatePullRequest	授予权限以在指定的存储库中创建拉取请求	Write	repository*		
CreatePullRequestApprovalRule	授予权限以创建特定于单个拉取请求的批准规则；不授予创建批准规则模板的权限	写入	repository*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateRepository	授予创建 Amazon CodeCommit 仓库的权限	写入	repository*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUnreferencedMergeCommit	授予权限以创建未引用的提交，其中包含使用三向或压缩合并选项合并两个提交的结果；不控制 Git 合并操作	Write	repository*		
				codecommit:References	
DeleteApprovalRuleTemplate	授予权限以删除批准规则模板	写入			
DeleteBranch	授予使用此 API 删除 Amazon CodeCommit 仓库中分支的权限；不控制 Git 删除分支操作	写入	repository*		
				codecommit:References	
DeleteCommentContent	授予权限以删除对存储库中的更改、文件或提交进行的评论内容	Write	repository*		
DeleteFile	授予权限以从指定的分支中删除指定的文件	Write	repository*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				codecommit:References	
DeletePullRequestApprovalRule	授予权限以删除为拉取请求创建的批准规则（如果该规则不是由批准规则模板创建）	写入	repository*		
DeleteRepository	授予删除 Amazon CodeCommit 仓库的权限	写入	repository*		
DescribeMergeConflicts	授予权限以获取有关在尝试使用三向或压缩合并选项合并两个提交时发生的特定合并冲突的信息	Read	repository*		
DescribePullRequestEvents	授予权限以返回有关一个或多个拉取请求事件的信息	Read	repository*		
DisassociateApprovalRuleTemplateFromRepository	授予权限以删除批准规则模板与存储库之间关联	Write	repository*		
EvaluatePullRequestApprovalRules	授予权限以根据拉取请求的当前批准状态和批准规则要求评估拉取请求是否可合并	Read	repository*		
GetApprovalRuleTemplate	授予权限以返回有关批准规则模板的信息	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetBlob	授予从控制台查看 Amazon CodeCommit 存储库中单个文件的编码内容的 Amazon CodeCommit 权限	读取	repository*		
GetBranch	授予使用此 API 获取 Amazon CodeCommit 仓库中分支详细信息的权限；不控制 Git 分支操作	读取	repository*		
GetComment	授予权限以获取对存储库中的更改、文件或提交进行的评论内容	Read	repository*		
GetCommentReactions	授予权限以获取对评论的反应	Read	repository*		
GetCommentsForComparedCommit	授予权限以获取有关对两次提交的比较结果进行的评论的信息	Read	repository*		
GetCommentsForPullRequest	授予权限以获取对拉取请求进行的评论	Read	repository*		
GetCommit	授予权限以使用该 API 返回有关提交的信息，包括提交消息和提交者信息；不控制 Git 日志操作	Read	repository*		
GetCommitHistory[仅权限]	授予权限以获取有关存储库中的提交历史记录的信息	Read	repository*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetCommitsFromMergeBase[仅权限]	授予权限以获取有关潜在合并上下文中的两次提交之间差异的信息	Read	repository*		
GetDifferences	授予权限以查看有关有效提交说明符（例如分支、标签、HEAD、提交 ID 或其他完全限定的引用）之间差异的信息	Read	repository*		
GetFile	授予权限以返回指定文件及其元数据的 Base-64 编码内容	Read	repository*		
GetFolder	授予权限以返回存储库中的指定文件夹的内容	Read	repository*		
GetMergeCommit	授予权限以获取有关创建合并提交的拉取请求合并选项之一创建的合并提交的信息。并非所有合并选项都创建合并提交。该权限不控制 Git 合并操作	读取	repository*		
				codecommit:References	
GetMergeConflicts	授予权限以获取有关仓库中拉取请求提交前和提交 IDs 后合并冲突的信息	读取	repository*		
GetMergeOptions	授予权限以获取有关可用于合并两个提交的拉取请求合并选项的信息；不控制 Git 合并操作	Read	repository*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetObjectIdentifier[仅权限]	授予权限以将 Blob、树和提交解析为其标识符	Read	repository*		
GetPullRequest	授予权限以获取有关指定存储库中的拉取请求的信息	Read	repository*		
GetPullRequestApprovalStates	授予权限以在输入的拉取请求上检索当前的批准	Read	repository*		
GetPullRequestOverrideState	授予权限以检索给定拉取请求的当前覆盖状态	Read	repository*		
GetReferences[仅权限]	授予获取 Amazon CodeCommit 仓库中引用详细信息的权限；不控制 Git 引用操作	读取	repository*		
GetRepository	授予获取 Amazon CodeCommit 仓库信息的权限	读取	repository*		
GetRepositoryTriggers	授予权限以获取有关为存储库配置的触发器的信息	Read	repository*		
GetTree[仅权限]	授予从 Amazon CodeCommit 控制台查看 Amazon CodeCommit 存储库中指定树内容的权限	读取	repository*		
GetUploadArchiveStatus[仅权限]	授予权限以获取有关上传到管道的档案的状态信息 Amazon CodePipeline	读取	repository*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GitPull[仅权限]	授予将信息从 Amazon CodeCommit 存储库提取到本地存储库的权限	读取	repository*		
GitPush[仅权限]	授予将信息从本地存储库推送到存储库的 Amazon CodeCommit 权限	写入	repository*		
				codecommit:References	
ListApprovalRuleTemplates	授予在中列出所有批准规则模板 Amazon Web Services 区域的权限 Amazon Web Services 账户	列表			
ListAssociatedApprovalRuleTemplatesForRepository	授予权限以列出与存储库关联的批准规则模板	列表	repository*		
ListBranches	授予使用此 API 列出 Amazon CodeCommit 仓库分支的权限；不控制 Git 分支操作	列表	repository*		
ListFileCommitHistory	授予列出对指定文件的提交和更改的权限	列表	repository*		
ListPullRequests	授予权限以列出指定存储库的拉取请求	列表	repository*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListRepositories	授予您列出当前区域中 Amazon CodeCommit 仓库信息的权限 Amazon Web Services 账户	列表			
ListRepositoriesForApprovalRuleTemplate	授予权限以列出与批准规则模板关联的存储库	列表			
ListTagsForResource	授予列出附加到资源 ARN 的 CodeCommit 资源的权限	列表	repository		
MergeBranchesByFastForward	授予权限以使用快进合并选项将两个提交合并到指定的目标分支中	Write	repository*		
				codecommit:References	
MergeBranchesBySquash	授予权限以使用压缩合并选项将两个提交合并到指定的目标分支中	Write	repository*		
				codecommit:References	
MergeBranchesByThreeWay	授予权限以使用三向合并选项将两个提交合并到指定的目标分支中	Write	repository*		
				codecommit:References	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
MergePullRequestByFastForward	授予权限以关闭拉取请求，并尝试使用快进合并选项将其合并到指定提交中的该拉取请求的指定目标分支中	Write	repository*		
				codecommit:References	
MergePullRequestBySquash	授予权限以关闭拉取请求，并尝试使用压缩合并选项将其合并到指定提交中的该拉取请求的指定目标分支中	Write	repository*		
				codecommit:References	
MergePullRequestByThreeWay	授予权限以关闭拉取请求，并尝试使用三向合并选项将其合并到指定提交中的该拉取请求的指定目标分支中	Write	repository*		
				codecommit:References	
OverridePullRequestApprovalRules	授予权限以覆盖某个拉取请求的所有批准规则，包括由模板创建的批准规则	Write	repository*		
PostCommentForComparedCommit	授予权限以对两个提交之间的比较结果发布评论	Write	repository*		
PostCommentForPullRequest	授予权限以对拉取请求发布评论	Write	repository*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PostCommentReply	授予权限以发布评论，以便回复对提交之间的比较结果或拉取请求进行的评论	Write	repository*		
PutCommentReaction	授予权限以对评论发布反应	写入	repository*		
PutFile	授予在 Amazon CodeCommit 存储库分支中添加或更新文件的权限，以及为指定分支中的新增文件生成提交	写入	repository*		
				codecommit:References	
PutRepositoryTriggers	授予权限以创建、更新或删除存储库的触发器	写入	repository*		
TagResource	授予将资源标签附加到 CodeCommit 资源 ARN 的权限	标记	repository		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
TestRepositoryTriggers	授予权限以将信息发送到触发器目标，以便测试存储库触发器的功能	写入	repository*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UntagResource	授予取消资源标签与资源 ARN 关联的 CodeCommit 权限	标记	repository		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateApprovalRuleTemplateContent	授予权限以更新批准规则模板内容；不授予更新专为拉取请求创建的批准规则内容的权限	Write			
UpdateApprovalRuleTemplateDescription	授予权限以更新批准规则模板的描述	Write			
UpdateApprovalRuleTemplateName	授予权限以更新批准规则模板的名称	Write			
UpdateComment	授予权限以在身份与用于创建评论的身份匹配时更新评论内容	写入	repository*		
UpdateDefaultBranch	授予更改 Amazon CodeCommit 仓库中默认分支的权限	写入	repository*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdatePullRequestApprovalRuleContent	授予权限以更新为特定拉取请求创建的批准规则内容；不授予更新使用批准规则模板为规则创建的批准规则内容的权限	Write	repository*		
UpdatePullRequestApprovalState	授予权限以更新拉取请求的批准状态	Write	repository*		
UpdatePullRequestDescription	授予权限以更新拉取请求描述	Write	repository*		
UpdatePullRequestStatus	授予权限以更新拉取请求状态	Write	repository*		
UpdatePullRequestTitle	授予权限以更新推送请求标题	写入	repository*		
UpdateRepositoryDescription	授予更改 Amazon CodeCommit 仓库描述的权限	写入	repository*		
UpdateRepositoryEncryptionKey	授予更改用于加密和解密存储库的 Amazon KMS 加密密钥的权限 Amazon CodeCommit	写入	repository*		
UpdateRepositoryName	授予更改 Amazon CodeCommit 仓库名称的权限	写入	repository*		
UploadArchive[仅权限]	向的服务角色授予将仓库变更上传 Amazon CodePipeline 到管道的权限	写入	repository*		

Amazon CodeCommit 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
repository	arn:${Partition}:codecommit:${Region}:${Account}:${RepositoryName}	aws:ResourceTag/${TagKey}

Amazon CodeCommit 的条件键

Amazon CodeCommit 定义了可在 IAM 策略Condition元素中使用的以下条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对来筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按附加到资源的标签键值对筛选操作	字符串
aws:TagKeys	根据在请求中是否具有标签键来筛选访问	ArrayOfString
codecommit:References	通过 Git 对指定 Amazon CodeCommit 操作的引用筛选访问权限	字符串

Amazon CodeDeploy 的操作、资源和条件键

Amazon CodeDeploy （服务前缀:codedeploy）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon CodeDeploy 定义的操作
- Amazon CodeDeploy 定义的资源类型
- Amazon CodeDeploy 的条件键

Amazon CodeDeploy 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddTagsToOnPremisesInstances	授予权限以向一个或多个本地部署实例添加标签	标记	instance*		
BatchGetApplicationRevisions	授予权限以获取有关一个或多个应用程序修订的信息	读取	application*		
BatchGetApplications	授予权限以获取有关与 IAM 用户关联的多个应用程序的信息	读取	application*		
BatchGetDeploymentGroups	授予权限以获取有关一个或多个部署组的信息	读取	deploymentgroup*		
BatchGetDeploymentInstances	授予权限以获取有关属于部署组的一个或多个实例的信息	读取	deploymentgroup*		
BatchGetDeploymentTargets	授予权限以返回与部署关联的一个或多个目标的数组。此方法适用于所有计算类型，应使用该方法代替已弃用的 BatchGetDeploymentInstances方法。可以返回的最大目标数量为 25	读取			
BatchGetDeployments	授予权限以获取有关与 IAM 用户关联的多个部署的信息	读取	deploymentgroup*		
BatchGetOnPremisesInstances	授予权限以获取有关一个或多个本地实例的信息	读取	instance*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ContinueDeployment	授予权限以启动将来自原始环境中的实例的流量重新路由到替换环境中的实例的过程，而无需等待指定的等待时间过去	写入			
CreateApplication	授予权限以创建与 IAM 用户关联的应用程序	写入	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudFormationDeployment[仅权限]	授予创建 CloudFormation 部署以合作管理堆栈更新的 CloudFormation 权限	写入			
CreateDeployment	授予权限以创建与 IAM 用户关联的应用程序部署	写入	deploymentgroup*		
CreateDeploymentConfig	授予权限以创建与 IAM 用户关联的自定义部署配置	写入	deploymentconfig*		
CreateDeploymentGroup	授予权限以创建与 IAM 用户关联的应用程序部署组	写入	deploymentgroup*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	授予权限以删除与 IAM 用户关联的应用程序	写入	application*		
DeleteDeploymentConfig	授予权限以删除与 IAM 用户关联的自定义部署配置	写入	deploymentconfig*		
DeleteDeploymentGroup	授予权限以删除与 IAM 用户关联的应用程序部署组	写入	deploymentgroup*		
DeleteGitHubAccountToken	授予删除 GitHub 账户连接的权限	写入			
DeleteResourcesByExternalId	授予权限以删除与给定外部 ID 关联的资源	写入			
DeregisterOnPremisesInstance	授予权限以注销本地部署的实例	写入	instance*		
GetApplication	授予权限以获取有关与 IAM 用户关联的单个应用程序的信息	列表	application*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetApplicationRevision	授予权限以获取有关与 IAM 用户关联的应用程序的单个应用程序修订的信息	列表	application*		
GetDeployment	授予权限以获取有关与 IAM 用户关联的应用程序的部署组的单个部署的信息	列表	deploymentgroup*		
GetDeploymentConfig	授予权限以获取有关与 IAM 用户关联的单个部署配置的信息	列表	deploymentconfig*		
GetDeploymentGroup	授予权限以获取有关与 IAM 用户关联的应用程序的单个部署组的信息	列表	deploymentgroup*		
GetDeploymentInstance	授予权限以获取有关部署中与 IAM 用户关联的单个实例的信息	列表	deploymentgroup*		
GetDeploymentTarget	授予权限以返回有关部署目标的信息	读取			
GetOnPremisesInstance	授予权限以获取有关单个本地部署实例的信息	列表	instance*		
ListApplicationRevisions	授予权限以获取有关与 IAM 用户关联的应用程序的所有应用程序修订的信息	列表	application*		
ListApplications	授予权限以获取有关与 IAM 用户关联的所有应用程序的信息	列表			
ListDeploymentConfigs	授予权限以获取有关与 IAM 用户关联的所有部署配置的信息	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListDeploymentGroups	授予权限以获取有关与 IAM 用户关联的应用程序的所有部署组的信息	列表	application*		
ListDeploymentInstances	授予权限以获取有关部署中与 IAM 用户关联的所有实例的信息	列表	deploymentgroup*		
ListDeploymentTargets	授予返回与部署关联 IDs 的目标数组的权限	列表			
ListDeployments	授予权限以获取有关与 IAM 用户关联的部署组的所有部署的信息，或获取与 IAM 用户关联的所有部署	列表	deploymentgroup*		
ListGitHubAccountTokenNames	授予列出 GitHub 账户存储连接名称的权限	列表			
ListOnPremisesInstances	授予权限以获取一个或多个本地实例名称的列表	列表			
ListTagsForResource	授予权限以返回由指定 ARN 标识的资源的标签列表。标签用于对您的 CodeDeploy 资源进行组织和分类	列表	application deploymentgroup		
PutLifecycleEventHookExecutionStatus	授予权限以通知与 IAM 用户关联的部署的生命周期事件挂钩执行状态	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
RegisterApplicationRevision	授予权限以注册有关与 IAM 用户关联的应用程序的应用程序修订的信息	写入	application*		
RegisterOnPremisesInstance	授予权限以注册本地部署的实例	写入	instance*		
RemoveTagsFromOnPremisesInstances	授予权限以从一个或多个本地部署实例移除标签	标记	instance*		
SkipWaitTimeForInstanceTermination	授予权限以覆盖任何指定的等待时间，并在流量路由完成后立即开始终止实例。此操作仅适用于蓝-绿部署	写入			
StopDeployment	授予停止部署的权限	写入			
TagResource	授予将输入 Tags 参数中的标签列表与输入参数标识的资源关联的 ResourceArn 权限	标记	application		
			deploymentgroup		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UntagResource	授予权限以从一系列标签中取消与资源的关联。资源由 ResourceArn 输入参数标识。标签由输入参数中的密钥列表标 TagKeys 识	标记	application		
			deploymentgroup		
				aws:TagKeys	
UpdateApplication	授予更新应用程序的权限	写入	application*		
UpdateDeploymentGroup	授予权限以更改有关与 IAM 用户关联的应用程序的单个部署组的信息	写入	deploymentgroup*		

Amazon CodeDeploy 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
application	arn:${Partition}:codedeploy:${Region}:${Account}:application:${ApplicationName}	aws:ResourceTag/${TagKey}
deploymentconfig	arn:${Partition}:codedeploy:${Region}:${Account}:deploymentconfig:${DeploymentConfigurationName}	

资源类型	ARN	条件键
deploymentgroup	arn:${Partition}:codedeploy:${Region}:${Account}:deploymentgroup:${ApplicationName}/${DeploymentGroupName}	aws:ResourceTag/${TagKey}
instance	arn:${Partition}:codedeploy:${Region}:${Account}:instance:${InstanceName}	

Amazon CodeDeploy 的条件键

Amazon CodeDeploy 定义了可在 IAM 策略Condition元素中使用的以下条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对以筛选操作	字符串
aws:ResourceTag/${TagKey}	根据附加到资源的标签键值对筛选操作	字符串
aws:TagKeys	根据在请求中是否具有标签键以筛选操作	ArrayOfString

Amazon CodeDeploy 安全主机命令服务的操作、资源和条件密钥

Amazon CodeDeploy secure host 命令服务（服务前缀:codedeploy-commands-secure）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。

- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

由 Amazon CodeDeploy 安全主机命令服务定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetDeploymentSpecification	授予获取部署规范的权限	读取			
PollHostCommand	授予请求主机代理命令的权限	读取			
PutHostCommandAcknowledgement	授予权限以将主机代理命令标记为已确认	写入			
PutHostCommandComplete	授予权限以将主机代理命令标记为已完成	写入			

由 Amazon CodeDeploy 安全主机命令服务定义的资源类型

Amazon CodeDeploy 安全主机命令服务不支持在 IAM 策略声明的`Resource`元素中指定资源 ARN。要允许访问 Amazon CodeDeploy 安全主机命令服务，请在策略`"Resource": "*"`中指定。

Amazon CodeDeploy 安全主机命令服务的条件密钥

CodeDeploy Commands Secure 没有可在策略声明`Condition`元素中使用的特定于服务的上下文密钥。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon CodePipeline 的操作、资源和条件键

Amazon CodePipeline（服务前缀:`codepipeline`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。

- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon CodePipeline 定义的操作
- Amazon CodePipeline 定义的资源类型
- Amazon CodePipeline 的条件键

Amazon CodePipeline 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AcknowledgeJob	授予查看有关指定作业的信息以及作业工作线程是否已收到该作业的权限	Write			
AcknowledgeThirdPartyJob	授予确认作业工作线程是否已收到指定作业的权限（仅限合作伙伴操作）	写入			
CreateCustomActionType	授予创建自定义操作的权限，您可以在与您的关联的管道中使用该操作 Amazon Web Services 账户	写入	actiontype*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePipeline	授予权限以创建唯一命名管道	写入	pipeline*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCustomActionType	授予权限以删除自定义操作	Write	actiontype*		
DeletePipeline	授予删除指定管道的权限	Write	pipeline*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteWebhook	授予删除指定 Webhook 的权限	Write	webhook*		
DeregisterWebhookWithThirdParty	授予删除在其配置中指定了第三方的 Webhook 的注册权限	Write	webhook*		
DisableStageTransition	授予阻止修订过渡到管道中的下一个阶段的权限	Write	stage*		
EnableStageTransition	授予允许修订过渡到管道中的下一阶段的权限	写入	stage*		
GetActionType	授予权限以查看有关操作类型的信息	读取			
GetJobDetails	授予权限以查看任务相关信息（仅自定义操作）	Read			
GetPipeline	授予检索管道结构相关信息的权限	Read	pipeline*		
GetPipelineExecution	授予查看管道执行信息的权限，这些信息包括有关构件的详细信息、管道执行 ID 以及管道的名称、版本和状态。	Read	pipeline*		
GetPipelineState	授予查看管道阶段和操作的当前状态信息的权限	Read	pipeline*		
GetThirdPartyJobDetails	授予查看第三方操作的作业详细信息的权限（仅限合作伙伴操作）	Read			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListActionExecutions	授予列出管道中发生的操作执行的权限	Read	pipeline*		
ListActionTypes	授予列出账户中管道的所有可用操作类型摘要的权限	Read			
ListPipelineExecutions	授予列出管道的最近执行摘要的权限	列表	pipeline*		
ListPipelines	授予列出与您关联的所有管道摘要的权限 Amazon Web Services 账户	列表			
ListRuleExecutions	授予权限以列出管道中发生的规则执行	读取	pipeline*		
ListRuleTypes	授予权限以列出账户中管道的所有可用规则类型摘要	读取			
ListTagsForResource	授予列出 CodePipeline 资源标签的权限	读取	actiontype		
			pipeline		
			webhook		
ListWebhooks	授予列出与你关联的所有 webhook 的权限 Amazon Web Services 账户	列表	webhook*		
OverrideStageCondition	授予权限以通过重写阶段条件来恢复管道执行	写入	stage*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PollForJobs	授予权限以查看有关任何 CodePipeline 要处理的任务的信息	写入	actiontype*		
PollForThirdPartyJobs	授予确定是否存在任何可供作业工作线程执行操作的第三方作业的权限（仅限合作伙伴操作）	Write			
PutActionRevision	授予编辑管道中操作的权限	写入	action*		
PutApprovalResult	授予对手动批准请求作出回应（已批准或已拒绝）的权限 CodePipeline	写入	action*		
PutJobFailureResult	授予表示作业工作线程返回给管道的作业失败的权限（仅限自定义操作）	Write			
PutJobSuccessResult	授予表示作业工作线程返回给管道的作业成功的权限（仅限自定义操作）	Write			
PutThirdPartyJobFailureResult	授予表示作业工作线程返回给管道的第三方作业失败的权限（仅限合作伙伴操作）	Write			
PutThirdPartyJobSuccessResult	授予表示作业工作线程返回给管道的第三方作业成功的权限（仅限合作伙伴操作）	Write			
PutWebhook	授予权限以创建或更新 Webhook	写入	pipeline*		
			webhook*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
RegisterWebhookWithThirdParty	授予权限以注册在其配置中指定了第三方的 Webhook	Write	webhook*		
RetryStageExecution	授予通过重试阶段中最后一个失败的操作来恢复管道执行的权限	写入	stage*		
RollbackStage	授予权限以将阶段回滚到之前的成功执行	写入	stage*		
StartPipelineExecution	授予通过管道运行最新修订的权限	Write	pipeline*		
StopPipelineExecution	授予停止正在进行的管道执行的权限	写入	pipeline*		
TagResource	授予标记 CodePipeline 资源的权限	标记	actiontype		
			pipeline		
			webhook		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予从 CodePipeline 资源中移除标签的权限	标记	actiontype		
			pipeline		
			webhook		
				aws:TagKeys	
UpdateActionType	授予权限以更新操作类型	写入	actiontype*		
UpdatePipeline	授予权限以通过更改管道结构来更新管道	写入	pipeline*		

Amazon CodePipeline 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
action	arn:${Partition}:codepipeline:${Region}:${Account}:${PipelineName}/${StageName}/${ActionName}	aws:ResourceTag/${TagKey}
actiontype	arn:${Partition}:codepipeline:${Region}:${Account}:actiontype:${Owner}/${Category}/${Provider}/${Version}	aws:ResourceTag/${TagKey}
pipeline	arn:${Partition}:codepipeline:${Region}:${Account}:${PipelineName}	aws:ResourceTag/${TagKey}
stage	arn:${Partition}:codepipeline:${Region}:${Account}:${PipelineName}/${StageName}	aws:ResourceTag/${TagKey}
webhook	arn:${Partition}:codepipeline:${Region}:${Account}:webhook:${WebhookName}	aws:ResourceTag/${TagKey}

Amazon CodePipeline 的条件键

Amazon CodePipeline 定义了可在 IAM 策略Condition元素中使用的以下条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对以筛选操作	字符串
aws:ResourceTag/${TagKey}	根据附加到资源的标签键值对筛选操作	字符串
aws:TagKeys	根据在请求中是否具有标签键以筛选操作	ArrayOfString

Amazon Cognito Identity 的操作、资源和条件键

Amazon Cognito Identity（服务前缀：cognito-identity）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon Cognito Identity 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateIdentityPool	授予权限以创建新的身份池	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteIdentities	授予权限以从身份池中删除身份。您可以指定希望删除的 1-60 个身份的列表	Write			
DeleteIdentityPool	授予权限以删除用户池。将池删除后，用户将无法使用该池进行身份验证	Write	identitypool*		
DescribeIdentity	授予权限以返回与给定身份相关的元数据，包括创建身份的时间以及所有相关的关联登录名	Read			
DescribeIdentityPool	授予权限以获得特定身份池的详细信息，包括池名称、ID 描述、创建日期和当前用户数量	Read	identitypool*		
GetCredentialsForIdentity	授予权限以返回所提供身份 ID 的凭证	Read			
GetId	授予权限以生成（或检索）Cognito ID 提供多个登录名将创建隐式关联的账户	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetIdentityPoolAnalytics	授予获取有关所有身份池身份提供商当前身份总数的分析数据的权限 (IdPs)	读取	identitypool*		
GetIdentityPoolDailyAnalytics	授予获取有关所有身份池身份提供商的新身份数量和总身份的分析数据的权限 (IdPs)	读取	identitypool*		
GetIdentityPoolRoles	授予权限以获取身份池的角色	读取	identitypool*		
GetIdentityProviderDailyAnalytics	授予获取有关一个身份池身份提供商的新身份数量和总身份的分析数据的权限 (IdPs)	读取	identitypool*		
GetOpenIdToken	授予权限以使用已知 Cognito ID 获取 OpenID 令牌	读取			
GetOpenIdTokenForDeveloperIdentity	向通过后端身份验证流程进行身份验证的用户授予注册（或检索）Cognito IdentityId 和 OpenID Connect 令牌的权限	读取	identitypool*		
GetPrincipalTagAttributeMap	授予权限以获取身份池和提供商的委托人标签	Read	identitypool*		
ListIdentities	授予权限以在身份池中列出身份	List	identitypool*		
ListIdentityPools	授予权限以列出为您的账户注册的所有 Cognito 身份池	List			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListTagsForResource	授予权限以列出分配给 Amazon Cognito 身份池的标签	读取	identitypool		
LookupDeveloperIdentity	授予权限以 IdentityId 检索与现有身份 DeveloperUserIdentifiers 关联的 DeveloperUserIdentifier 或与之关联 IdentityId 的列表	读取	identitypool*		
MergeDeveloperIdentities	授予权限以合并两个不同的用户 IdentityIds、存在于同一个身份池中并由同一个开发者提供商标识的用户	写入	identitypool*		
SetIdentityPoolRoles	授予权限以设置身份池的角色 这些角色用于发出号召性用 GetCredentialsForIdentity 语	写入			
SetPrincipalTagAttributeMap	授予权限以设置身份池和提供商的委托人标签 这些标签用于发出号召性用 GetOpenIdToken 语	写入			
TagResource	授予权限以将一组标签分配给 Amazon Cognito 身份池	标记	identitypool		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UnlinkDeveloperIdentity	授予取消与现有身份关联 DeveloperUserIdentifier 的权限	写入	identitypool*		
UnlinkIdentity	授予权限以将联合身份与现有账户取消关联	Write			
UntagResource	授予权限以从 Amazon Cognito 身份池中删除指定的标签	Tagging	identitypool		
				aws:TagKeys	
UpdateIdentityPool	授予权限以更新身份池	Write	identitypool*		

Amazon Cognito Identity 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
identitypool	arn:${Partition}:cognito-identity:${Region}:${Account}:identitypool/${IdentityPoolId}	aws:ResourceTag/${TagKey}

Amazon Cognito Identity 的条件键

Amazon Cognito Identity 定义以下可以在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对以筛选操作	字符串
aws:ResourceTag/${TagKey}	根据附加到资源的标签键值对筛选操作	字符串
aws:TagKeys	按请求中包含的键筛选访问	ArrayOfString

Amazon Compute Optimizer 的操作、资源和条件键

Amazon Compute Optimizer（服务前缀:`compute-optimizer`）提供以下特定于服务的资源、操作和条件上下文密钥，用于 IAM 权限策略。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Compute Optimizer 定义的操作
- Amazon Compute Optimizer 定义的资源类型
- Amazon Compute Optimizer 的条件键

Amazon Compute Optimizer 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，

以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteRecommendationPreferences	授予权限以删除建议首选项	写入		compute-optimizer:ResourceType	autoscaling:DescribeAutoScalingGroups ec2:DescribeInstances rds:DescribeDBClusters rds:DescribeDBInstances

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeRecommendationExportJobs	授予查看建议导出作业的状态的权限	列表			
ExportAutoScalingGroupRecommendations	授予将所提供账户的 AutoScaling 群组推荐导出到 S3 的权限	写入			autoscaling:DescribeAutoScalingGroups compute-optimizer:GetAutoScalingGroupRecommendations
ExportEBSVolumeRecommendations	授予为提供的账户将 EBS 卷建议导出到 S3 的权限	写入			compute-optimizer:GetEBSVolumeRecommendations ec2:DescribeVolumes

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ExportEC2InstanceRecommendations	授予将所提供账户的 EC2 实例建议导出到 S3 的权限	写入			compute-optimizer:GetEC2InstanceRecommendations ec2:DescribeInstances
ExportECSServiceRecommendations	授予为提供的账户将 ECS 服务建议导出到 S3 的权限	写入			compute-optimizer:GetECSServiceRecommendations ecs:ListClusters ecs:ListServices
ExportIdleRecommendations	授予将所提供账户的闲置推荐导出到 S3 的权限	写入			compute-optimizer:GetIdleRecommendations

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ExportLambdaFunctionRecommendations	授予为提供的账户将 Lambda 函数建议导出到 S3 的权限	写入			compute-optimizer:GetLambdaFunctionRecommendations lambda:ListFunctions lambda:ListProvisionedConcurrencyConfigs
ExportLicenseRecommendations	授予为提供的账户将许可证建议导出到 S3 的权限	写入			compute-optimizer:GetLicenseRecommendations ec2:DescribeInstances

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ExportRDSDatabaseRecommendations	授予权限以为提供的账户将 RDS 建议导出到 S3	写入			compute-optimizer:GetRDSDatabaseRecommendations rds:DescribeDBClusters rds:DescribeDBInstances
GetAutoScalingGroupRecommendations	授予获取所提供 AutoScaling 群组推荐的权限	列表			autoscaling:DescribeAutoScalingGroups
GetEBSVolumeRecommendations	授予为提供的 EBS 卷获取建议的权限	列表			ec2:DescribeVolumes
GetEC2InstanceRecommendations	授予获取所提供 EC2 实例推荐的权限	列表			ec2:DescribeInstances
GetEC2RecommendationProjectedMetrics	授予获取指定实例的建议投影指标的权限	列表			ec2:DescribeInstances

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetECSServiceRecommendationProjectedMetrics	授予获取指定 ECS 服务的建议预测指标的权限	列表			
GetECSServiceRecommendations	授予为提供的 ECS 服务获取建议的权限	列表			ecs:ListClusters ecs:ListServices

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetEffectiveRecommendationPreferences	授予获取有效的建议首选项的权限	读取		compute-optimizer:ResourceType	autoscaling:DescribeAutoScalingGroups autoscaling:DescribeAutoScalingInstances ec2:DescribeInstances rds:DescribeDBClusters rds:DescribeDBInstances
GetEnrollmentStatus	授予为指定账户获取注册状态的权限	列表			
GetEnrollmentStatusesForOrganization	授予权限以获取组织成员账户的注册状态	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetIdleRecommendations	授予获取指定账户闲置推荐的权限	列表			
GetLambdaFunctionRecommendations	授予为提供的 Lambda 函数获取建议的权限	列表			lambda:ListFunctions lambda:ListProvisionedConcurrencyConfigs
GetLicenseRecommendations	授予为指定账户获取许可证建议的权限	列表			ec2:DescribeInstances
GetRDSDatabaseRecommendationProjectedMetrics	授予获取指定实例的建议投影指标的权限	列表			rds:DescribeDBClusters rds:DescribeDBInstances
GetRDSDatabaseRecommendations	授予权限以为指定账户获取 RDS 建议	列表			rds:DescribeDBClusters rds:DescribeDBInstances

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetRecommendationPreferences	授予权限以获取建议首选项	读取		compute-optimizer:ResourceType	
GetRecommendationSummaries	授予为指定账户获取建议摘要的权限	列表			
PutRecommendationPreferences	授予权限以放置建议首选项	写入		compute-optimizer:ResourceType	autoscaling:DescribeAutoScalingGroups autoscaling:DescribeAutoScalingInstances ec2:DescribeInstances rds:DescribeDBClusters rds:DescribeDBInstances

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateEnrollmentStatus	授予更新注册状态的权限	Write			

Amazon Compute Optimizer 定义的资源类型

Amazon Compute Optimizer 不支持在 IAM 策略声明的`Resource`元素中指定资源 ARN。要允许访问 Amazon Compute Optimizer，请在策略中指定 `"Resource": "*"`。

Amazon Compute Optimizer 的条件键

Amazon Compute Optimizer 定义了以下可以在 IAM 策略`Condition`元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
compute-optimizer:ResourceType	按资源类型筛选访问权限	字符串

Amazon Config 的操作、资源和条件键

Amazon Config（服务前缀:`config`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Config 定义的操作
- Amazon Config 定义的资源类型
- Amazon Config 的条件键

Amazon Config 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateResourceTypes	授予将所有指定资源类型添加到 of 配置记录器的权限，并在录制时包括这些资源类型 RecordingGroup	写入	ConfigurationRecorder*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchGetAggregateResourceConfig	授予返回您的 C Amazon onfig 聚合器中存在的资源的当前配置项目的权限	读取	ConfigurationAggregator*		
BatchGetResourceConfig	授予为一个或多个请求资源返回当前配置的权限	Read			
DeleteAggregationAuthorization	授予在指定区域中删除向指定配置聚合器账户授予的授权的权限	写入	AggregationAuthorization*		
DeleteConfigRule	授予删除指定的 Amazon Config 规则及其所有评估结果的权限	写入	ConfigRule*		
DeleteConfigurationAggregator	授予删除指定的配置聚合器以及与聚合器关联的聚合数据的权限	写入	ConfigurationAggregator*		
DeleteConfigurationRecorder	授予删除客户托管配置记录器的权限	写入	ConfigurationRecorder*		
DeleteConformancePack	授予删除指定一致性包以及该一致性包中的所有 Amazon Config 规则和所有评估结果的权限	写入	ConformancePack*		
DeleteDeliveryChannel	授予删除配送通道的权限	Write			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteEvaluationResults	授予删除指定 Config 规则的评估结果的权限	Write	ConfigRule*		
DeleteOrganizationConfigRule	授予从该组织的所有成员账户中删除指定的组织 Config 规则及其所有评估结果的权限	Write	OrganizationConfigRule*		
DeleteOrganizationConformancePack	授予从该组织的所有成员账户中删除指定的组织一致性包及其所有评估结果的权限	Write	OrganizationConformancePack*		
DeletePendingAggregationRequest	授予在指定区域中删除指定聚合器账户的待处理授权请求的权限	Write			
DeleteRemediationConfiguration	授予删除修复配置的权限	写入	RemediationConfiguration*		
DeleteRemediationExceptions	授予删除特定 C Amazon onfig 规则中特定资源密钥的一个或多个修正例外的权限	写入			
DeleteResourceConfig	授予为已删除的自定义资源记录配置状态的权限	Write			
DeleteRetentionConfiguration	授予删除保留配置的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteServiceLinkedConfigurationRecorder	授予删除与服务相关的配置记录器的权限	写入	ConfigurationRecorder*		
				config:ConfigurationRecorderServicePrincipal	
DeleteStoredQuery	授予删除中存储的查询 Amazon Web Services 账户 的权限 Amazon Web Services 区域	写入	StoredQuery*		
DeliverConfigSnapshot	授予在指定的传输通道中计划将配置快照传输至 Amazon S3 存储桶的权限	Read			
DescribeAggregateComplianceByConfigRules	授予返回合规和不合规规则列表，以及合规和不合规规则的资源数的权限	Read	ConfigurationAggregator*		
DescribeAggregateComplianceByConformancePacks	授予返回合规和不合规一致性包列表以及每个一致性包中合规、不合规和总规则计数的权限	Read	ConfigurationAggregator*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeAggregationAuthorizations	授予返回授予各种聚合器账户和区域的授权列表的权限	列表			
DescribeComplianceByConfigRule	授予权限以指示指定的 Amazon Config 规则是否合规	读取			
DescribeComplianceByResource	授予指明指定 Amazon 资源是否合规的权限	读取			
DescribeConfigRuleEvaluationStatus	授予返回每条 Amazon 托管 Config 规则状态信息的权限	读取			
DescribeConfigRules	授予返回有关您的 Amazon Config 规则详细信息的权限	列表			
DescribeConfigurationAggregatorSourcesStatus	授予返回聚合器中源状态信息的权限	Read	ConfigurationAggregator*		
DescribeConfigurationAggregators	授予返回一个或多个配置聚合器详细信息的权限	List			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeConfigurationRecorderStatus	授予返回指定配置记录器的当前状态的权限	Read	ConfigurationRecorder*		
				config:ConfigurationRecorderServicePrincipal	
DescribeConfigurationRecorders	授予返回一个或多个指定配置记录器名称的权限	读取	ConfigurationRecorder*		
				config:ConfigurationRecorderServicePrincipal	
DescribeConformancePackCompliance	授予返回该一致性包中每个规则的合规性信息的权限	Read	ConformancePack*		
DescribeConformancePackStatus	授予提供一个或多个一致性包部署状态的权限	Read			
DescribeConformancePacks	授予返回一个或多个一致性包的列表的权限	List			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeDeliveryChannelStatus	授予返回指定传输通道的当前状态的权限	Read			
DescribeDeliveryChannels	授予返回有关指定传输通道的详细信息的权限	List			
DescribeOrganizationConfigRuleStatuses	授予为组织提供组织 Config 规则部署状态的权限	Read			
DescribeOrganizationConfigRules	授予返回组织 Config 规则列表的权限	List			
DescribeOrganizationConformancePackStatuses	授予为组织提供组织一致性包部署状态的权限	Read			
DescribeOrganizationConformancePacks	授予返回组织一致性包列表的权限	List			
DescribePendingAggregationRequests	授予返回所有待处理聚合请求列表的权限	List			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeRemediationConfigurations	授予返回一个或多个修复配置详细信息的权限	List	RemediationConfiguration*		
DescribeRemediationExceptions	授予返回一个或多个修复异常详细信息的权限	List			
DescribeRemediationExecutionStatus	授予提供一组资源的修复执行的详细视图（包括状态、时间戳以及失败步骤的任何错误消息）的权限	Read	RemediationConfiguration*		
DescribeRetentionConfigurations	授予返回一个或多个保留配置详细信息的权限	列表			
DisassociateResourceTypes	授予从配置记录器中删除所有指定资源类型的权限，并在录制时排除这些资源类型 RecordingGroup	写入	ConfigurationRecorder*		
GetAggregateComplianceDetailsByConfigRule	授予权限以返回规则中特定资源的指定 Amazon Config 规则的评估结果	读取	ConfigurationAggregator*		
GetAggregateConfigRuleComplianceSummary	授予返回聚合器中一个或多个账户和区域的合规和不合规规则数的权限	Read	ConfigurationAggregator*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetAggregateConformancePackComplianceSummary	授予返回聚合器中一个或多个账户和区域的合规和不合规一致性包数量的权限	读取	ConfigurationAggregator*		
GetAggregateDiscoveredResourceCounts	授予返回 C Amazon onfig 聚合器中存在的跨账户和区域的资源计数的权限	读取	ConfigurationAggregator*		
GetAggregateResourceConfig	授予返回在特定源账户和区域中为特定资源聚合的配置项的权限	读取	ConfigurationAggregator*		
GetComplianceDetailsByConfigRule	授予返回指定 Amazon Config 规则的评估结果的权限	读取	ConfigRule*		
GetComplianceDetailsByResource	授予返回指定 Amazon 资源的评估结果的权限	读取			
GetComplianceSummaryByConfigRule	授予返回合规和不合规的 Amazon Config 规则数量的权限，每条规则最多 25 个	读取			
GetComplianceSummaryByResourceType	授予返回合规和不合规的资源数量的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetConformancePackComplianceDetails	授予返回一致性包监控的所有 Amazon 资源的合规包合规性详细信息的权限	读取	ConformancePack*		
GetConformancePackComplianceSummary	授予为一个或多个一致性包提供合规性摘要的权限	读取	ConformancePack*		
GetCustomRulePolicy	授予返回包含 C Amazon onfig 自定义策略规则逻辑的策略定义的权限	读取	ConfigRule*		
GetDiscoveredResourceCounts	授予权限以返回 Config 在此区域中为您记录的资源类型、每种资源类型的数量以及 Amazon Config 记录的资源总数 Amazon Web Services 账户	读取			
GetOrganizationConfigRuleDetailedStatus	授予返回给定组织 Config 规则的组织内每个成员账户的详细状态的权限	Read	OrganizationConfigRule*		
GetOrganizationConformancePackDetailedStatus	授予返回给定组织一致性包的组织内每个成员账户的详细状态的权限	读取	OrganizationConformancePack*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetOrganizationCustomRulePolicy	授予返回包含组织逻辑的策略定义的权限 Amazon Config Custom Policy 规则规则	读取	OrganizationConfigRule*		
GetResourceConfigHistory	授予返回指定资源的配置项目列表的权限	读取			
GetResourceEvaluationSummary	授予返回特定资源评估 ID 的资源评估摘要的权限	读取			
GetStoredQuery	授予返回特定存储查询详细信息的权限	Read	StoredQuery*		
ListAggregateDiscoveredResources	授予接受资源类型，并返回在不同账户和区域中为特定资源类型聚合的资源标识符列表的权限	列表	ConfigurationAggregator*		
ListConfigurationRecorders	授予列出配置记录器摘要 Amazon Web Services 账户 的权限 Amazon Web Services 区域	列表			
ListConformancePackComplianceScores	授予权限以返回一致性包中合规规则-资源组合的百分比，该百分比与可能的规则-资源组合总数之比	列表			
ListDiscoveredResources	授予接受资源类型，并返回该类型资源的资源标识符列表的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListResourceEvaluations	授予列出资源评估摘要 Amazon Web Services 账户 的权限 Amazon Web Services 区域	列表			
ListStoredQueries	授予在中列出存储的查询 Amazon Web Services 账户 的权限 Amazon Web Services 区域	列表			
ListTagsForResource	授予列出 Amazon Config 资源标签的权限	读取	AggregationAuthorization		
			ConfigRule		
			ConfigurationAggregator		
			ConfigurationRecorder		
			ConformancePack		
			OrganizationConfigRule		
			OrganizationConformancePack		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			StoredQuery		
PutAggregationAuthorization	授予授权聚合器账户和区域从源账户和区域中收集数据的权限	写入	AggregationAuthorization*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutConfigRule	授予添加或更新用于评估您的 Amazon 资源是否符合所需 Amazon 配置的 Config 规则的权限	写入	ConfigRule*		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutConfigurationAggregator	授予使用所选源账户和区域创建和更新配置聚合器的权限	写入	ConfigurationAggregator*		iam:PassRole organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators
				aws:RequestTag/${TagKey} aws:TagKeys	
PutConfigurationRecorder	授予创建或更新客户管理的配置记录器以记录所选资源配置的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutConformancePack	授予创建或更新一致性包的权限	Write	ConformancePack*		iam:CreateServiceLinkedRole iam:PassRole s3:GetObject s3:ListBucket ssm:GetDocument
PutDeliveryChannel	授予创建传输通道对象，以将配置信息传输到 Amazon S3 存储桶和 Amazon SNS 主题的权限	写入			
PutEvaluations	授予 Amazon Lambda 函数用于向 Config 提供评估结果的权限 Amazon	写入			
PutExternalEvaluation	授予向 Amazon Config 传送评估结果的权限	写入	ConfigRule*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutOrganizationConfigRule	授予为整个组织添加或更新组织配置规则的权限，以评估您的 Amazon 资源是否符合所需的配置	写入	OrganizationConfigRule*		iam:CreateServiceLinkedRole iam:PassRole organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutOrganizationConformancePack	向整个组织授予添加或更新组织合规包的权限，以评估您的 Amazon 资源是否符合所需的配置	写入	OrganizationConformancePack*		iam:CreateServiceLinkedRole iam:PassRole organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators s3:GetObject
PutRemediationConfigurations	授予使用具有所选目标或操作的特定 Amazon Config 规则添加或更新修正配置的权限	写入	RemediationConfiguration*		iam:PassRole
PutRemediationExceptions	授予为特定 Amazon Config 规则添加或更新特定资源的修正例外情况的权限	写入			
PutResourceConfig	授予为请求中提供的资源记录配置状态的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutRetentionConfiguration	授予创建和更新保留配置的权限，其中包含有关 Amazon Config 存储您的历史信息的保留期（天数）的详细信息	写入			
PutServiceLinkedConfigurationRecorder	授予创建新的服务相关配置记录器的权限，以记录关联服务范围内的资源配置	写入		aws:RequestTag/${TagKey} aws:TagKeys config:ConfigurationRecorderServicePrincipal	iam:CreateServiceLinkedRole iam:PassRole
PutStoredQuery	授予保存新查询或更新现有已保存查询的权限	写入	StoredQuery*		
				aws:RequestTag/${TagKey} aws:TagKeys	
SelectAggregateResourceConfig	授予接受结构化查询语言 (SQL) SELECT 命令和聚合器的权限，以查询多个账户和地区的 Amazon 资源配置状态、执行相应的搜索并返回与属性匹配的资源配置	读取	ConfigurationAggregator*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
SelectResourceConfig	授予权限，以接受结构化查询语言 (SQL) SELECT 命令，执行相应的搜索，然后返回与属性匹配的资源配置	Read			
StartConfigRulesEvaluation	授予根据指定的 Config 规则评估资源的权限	写入	ConfigRule*		
StartConfigurationRecorder	向客户托管的配置记录器授予权限，允许其开始记录您选择记录在您的 Amazon 资源中的配置 Amazon Web Services 账户	写入	ConfigurationRecorder*		
StartRemediationExecution	授予针对上次已知的修复 Amazon 配置对指定的 Config 规则运行按需修复的权限	写入			iam:PassRole
StartResourceEvaluation	授予根据您账户中的 Amazon Config 规则评估您的资源详细信息的权限	写入			cloudformation:DescribeType
StopConfigurationRecorder	向客户托管的配置记录器授予权限，允许其停止记录您选择记录在您的 Amazon 资源中的配置 Amazon Web Services 账户	写入	ConfigurationRecorder*		
TagResource	授予使用指定 resourceArn 将指定标签关联到资源的权限	Tagging	AggregationAuthorization		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			ConfigRule		
			ConfigurationAggregator		
			ConfigurationRecorder		
			ConformancePack		
			OrganizationConfigRule		
			OrganizationConformancePack		
			StoredQuery		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予从资源中删除一个或多个标签的权限	Tagging	AggregationAuthorization		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			ConfigRule		
			ConfigurationAggregator		
			ConfigurationRecorder		
			ConformancePack		
			OrganizationConfigRule		
			OrganizationConformancePack		
			StoredQuery		
				aws:TagKeys	

Amazon Config 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
AggregationAuthorization	arn:${Partition}:config:${Region}:${Account}:aggregation-authorization/${AggregatorAccount}/${AggregatorRegion}	aws:ResourceTag/${TagKey}
ConfigurationAggregator	arn:${Partition}:config:${Region}:${Account}:config-aggregator/${AggregatorId}	aws:ResourceTag/${TagKey}
ConfigRule	arn:${Partition}:config:${Region}:${Account}:config-rule/${ConfigRuleId}	aws:ResourceTag/${TagKey}
ConformancePack	arn:${Partition}:config:${Region}:${Account}:conformance-pack/${ConformancePackName}/${ConformancePackId}	aws:ResourceTag/${TagKey}
OrganizationConfigRule	arn:${Partition}:config:${Region}:${Account}:organization-config-rule/${OrganizationConfigRuleId}	aws:ResourceTag/${TagKey}
OrganizationConformancePack	arn:${Partition}:config:${Region}:${Account}:organization-conformance-pack/${OrganizationConformancePackId}	aws:ResourceTag/${TagKey}
RemediationConfiguration	arn:${Partition}:config:${Region}:${Account}:remediation-configuration/${RemediationConfigurationId}	
StoredQuery	arn:${Partition}:config:${Region}:${Account}:stored-query/${StoredQueryName}/${StoredQueryId}	aws:ResourceTag/${TagKey}
ConfigurationRecorder	arn:${Partition}:config:${Region}:${Account}:configuration-recorder/${RecorderName}/${RecorderId}	aws:ResourceTag/${TagKey}

Amazon Config 的条件键

Amazon Config 定义了以下可以在 IAM 策略Condition元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按每个标签的允许值集筛选访问	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签值筛选访问权限	字符串
aws:TagKeys	按请求中是否具有必需标签来筛选访问	ArrayOfString
config:ConfigurationRecorderServicePrincipal	按配置记录器的服务主体筛选访问权限	字符串

Amazon Connector Service 的操作、资源和条件键

Amazon 连接器服务（服务前缀:awsconnector）提供以下特定于服务的资源、操作和条件上下文密钥，用于 IAM 权限策略。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Connector Service 定义的操作
- Amazon Connector Service 定义的资源类型

- Amazon Connector Service 的条件键

Amazon Connector Service 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetConnectorHealth[仅权限]	检索从服务器迁移连接器发布的所有运行状况指标。	Read			
RegisterConnector[仅权限]	向 Amazon 连接器服务注册 Amazon 连接器。	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ValidateConnectorId[仅权限]	验证在连接器服务中注册的服务器迁移 Amazon 连接器 ID。	读取			

Amazon Connector Service 定义的资源类型

Amazon 连接器服务不支持在 IAM 策略声明的`Resource`元素中指定资源 ARN。要允许对 Amazon Connector Service 的访问权限，请在策略中指定 `"Resource": "*"`。

Amazon Connector Service 的条件键

Connector Service 没有可在策略声明的 `Condition` 元素中使用的服务特定上下文键。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon 整合账单的操作、资源和条件键

Amazon 整合账单（服务前缀:`consolidatedbilling`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon 整合账单定义的操作
- Amazon 整合账单定义的资源类型
- Amazon 整合账单的条件键

Amazon 整合账单定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetAccountBillingRole[仅权限]	授予获取账户角色（付款人、关联角色、常规）的权限	读取			
ListLinkedAccounts[仅权限]	授予获取成员/关联账户列表的权限	列表			

Amazon 整合账单定义的资源类型

Amazon 整合账单不支持在 IAM 政策声明的Resource元素中指定资源 ARN。要允许访问 Amazon 整合账单，请在策略中指定 "Resource": "*"。

Amazon 整合账单的条件键

整合账单没有可在策略语句的 Condition 元素中使用的服务特定上下文键。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon 成本和使用情况报告的操作、资源和条件键

Amazon 成本和使用情况报告（服务前缀:cur）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon 成本和使用情况报告定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteReportDefinition	授予删除成本和使用情况报告定义的权限	写入	cur*		
DescribeReportDefinitions	授予获取成本和使用情况报告定义的权限	读取			
GetClassicReport[仅权限]	授予获取账单 CSV 报告的权限	读取			
GetClassicReportPreferences[仅权限]	授予获取使用情况报告的经典报告启用状态的权限	读取			
GetUsageReport[仅权限]	授予获取使用情况报告工作流程的 Amazon 服务、使用类型和操作列表的权限。同时允许或拒绝下载使用情况报告	读取			
ListTagsForResource	授予权限以列出资源的标签	读取	cur*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey}	
ModifyReportDefinition	授予修改成本和使用情况报告定义的权限	写入	cur*		
PutClassicReportPreferences[仅权限]	授予启用经典报告的权限	写入			
PutReportDefinition	授予编写成本和使用情况报告定义的权限	写入	cur*		
TagResource	授予权限以标记资源	Tagging	cur*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	授予权限以取消标记资源	Tagging	cur*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys aws:ResourceTag/${TagKey}	
ValidateReportDestination[仅权限]	授予验证是否存在具有适当 CUR 传递权限的 s3 桶的权限	读取			

Amazon 成本和使用情况报告定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
cur	arn:${Partition}:cur:${Region}:${Account}:definition/${ReportName}	

Amazon 成本和使用情况报告的条件键

Amazon 成本和使用情况报告定义了以下可用于 IAM 策略Condition元素的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString

Amazon Cost Explorer Service 的操作、资源和条件键

Amazon Cost Explorer 服务（服务前缀:ce）提供以下特定于服务的资源、操作和条件上下文密钥，用于 IAM 权限策略。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Cost Explorer Service 定义的操作
- Amazon Cost Explorer Service 定义的资源类型
- Amazon Cost Explorer Service 的条件键

Amazon Cost Explorer Service 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，

以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateAnomalyMonitor	授予权限以创建新的异常监控	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAnomalySubscription	授予权限以创建新的异常订阅	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCostCategoryDefinition	授予权限以创建具有请求的名称和规则的新成本类别	Write		aws:RequestTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys	
CreateNotificationSubscription[仅权限]	授予创建预留到期提醒的权限	Write			
CreateReport[仅权限]	授予创建 Cost Explorer 报告的权限	Write			
DeleteAnomalyMonitor	授予权限以删除异常监控	Write	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
DeleteAnomalySubscription	授予权限以删除异常订阅	Write	anomalysubscription*		
				aws:ResourceTag/${TagKey}	
DeleteCostCategoryDefinition	授予权限以删除成本类别	Write	costcategory*		
				aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteNotificationSubscription[仅权限]	授予删除预留到期提醒的权限	Write			
DeleteReport[仅权限]	授予删除 Cost Explorer 报告的权限	Write			
DescribeCostCategoryDefinition	授予权限以检索成本类别的名称、ARN、规则、定义和生效日期等描述	Read	costcategory*		
				aws:ResourceTag/${TagKey}	
DescribeNotificationSubscription[仅权限]	授予查看预留到期提醒的权限	Read			
DescribeReport[仅权限]	授予查看 Cost Explorer 报告页面的权限	Read			
GetAnomalies	授予权限以检索异常	Read	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
GetAnomalyMonitors	授予权限以查询异常监控	Read	anomalymonitor*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey}	
GetAnomalySubscriptions	授予权限以查询异常订阅	读取	anomalysubscription*		
				aws:ResourceTag/${TagKey}	
GetApproximateUsageRecords	授予权限以检索选定资源、级别和每小时粒度首选项的大致使用记录计数（源自上个月的使用情况）	读取			
GetCommitmentPurchaseAnalysis	授予检索您账户的承诺购买分析的权限	读取			
GetConsoleActionSetEnforced[仅权限]	授予权限以查看是否使用现有或精细的 IAM 操作来控制对账单、成本管理和账户控制台的授权	读取			
GetCostAndUsage	授予权限以检索您的账户的成本和使用率指标	Read	billingview		
				aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetCostAndUsageWithResources	授予权限以检索您的账户资源的成本和使用率指标	Read	billingview		
				aws:ResourceTag/${TagKey}	
GetCostCategories	授予查询指定时间段内 Cost Catagory 名称和值的权限	Read	billingview		
				aws:ResourceTag/${TagKey}	
GetCostForecast	授予权限以检索预测时间段的成本预测	Read	billingview		
				aws:ResourceTag/${TagKey}	
GetDimensionValues	授予权限以检索筛选条件在一段时间内的所有可用筛选条件值	Read	billingview		
				aws:ResourceTag/${TagKey}	
GetPreferences[仅权限]	授予查看“Cost Explorer 首选项”页面的权限	Read			
GetReservationCoverage	授予权限以检索您的账户的预留范围	Read			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetReservationPurchaseRecommendation	授予权限以检索您的账户的预留建议	Read			
GetReservationUtilization	授予权限以检索您的账户的预留利用率	Read			
GetRightsizingRecommendation	授予权限以检索您的账户的合理调整大小建议	读取			
GetSavingsPlanPurchaseRecommendationDetails	授予权限以检索账户的实惠配套建议详细信息	读取			
GetSavingsPlansCoverage	授予权限以检索您账户的 Savings Plans 覆盖范围	Read			
GetSavingsPlansPurchaseRecommendation	授予权限以检索您账户的 Savings Plans 建议	Read			
GetSavingsPlansUtilization	授予权限以检索您账户的 Savings Plans 利用率	Read			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetSavingsPlansUtilizationDetails	授予权限以检索您账户的 Savings Plans 利用率详细信息	Read			
GetTags	授予权限以查询指定时间段的标签	Read	billingview		
				aws:ResourceTag/${TagKey}	
GetUsageForecast	授予权限以检索预测时间段的使用情况预测	读取	billingview		
				aws:ResourceTag/${TagKey}	
ListCommitmentPurchaseAnalyses	授予检索历史承诺购买分析列表的权限	列表			
ListCostAllocationTagBackfillHistory	授予权限以列出成本分配标签回填历史记录	列表			
ListCostAllocationTags	授予列出成本分配标签的权限	列表			
ListCostCategoryDefinitions	授予权限以检索所有 Cost Categories 的名称、ARN 和生效日期	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListSavingsPlansPurchaseRecommendationGeneration	授予权限以检索您的历史建议生成列表	列表			
ListTagsForResource	授予列示 Cost Explorer 资源标签的权限	读取	anomalymonitor		
			anomalysubscription		
			costcategory		
				aws:ResourceTag/${TagKey}	
ProvideAnomalyFeedback	授予权限以提供对检测到的异常的反馈	写入			
StartCommitmentPurchaseAnalysis	授予请求承诺购买分析的权限	写入			
StartCostAllocationTagBackfill	授予权限以请求成本分配标签回填	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StartSavingsPlansPurchaseRecommendationGeneration	授予权限以请求 Savings Plans 建议生成	写入			
TagResource	授予标记 Cost Explorer 资源的权限	标记	anomalymonitor		
			anomalysubscription		
			costcategory		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	授予从 Cost Explorer 资源中删除标签的权限	标记	anomalymonitor		
			anomalysubscription		
			costcategory		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateAnomalyMonitor	授予权限以更新现有异常监控	Write	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
UpdateAnomalySubscription	授予权限以更新现有异常订阅	写入	anomalysubscription*		
				aws:ResourceTag/${TagKey}	
UpdateConsoleActionSetEnforced[仅权限]	授予权限以更改是使用现有还是精细的 IAM 操作来控制对账单、成本管理和账户控制台的授权	写入			
UpdateCostAllocationTagsStatus	授予更新现有成本分配标签状态的权限	写入			
UpdateCostCategoryDefinition	授予权限以更新现有成本类别	Write	costcategory*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey}	
UpdateNotificationSubscription[仅权限]	授予更新预留到期提醒的权限	Write			
UpdatePreferences[仅权限]	授予编辑“Cost Explorer 首选项”页的权限	Write			
UpdateReport[仅权限]	授予更新 Cost Explorer 报告的权限	Write			

Amazon Cost Explorer Service 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}

资源类型	ARN	条件键
billingview	arn:${Partition}:billing::${Account}:billingview/${ResourceId}	aws:ResourceTag/${TagKey}

Amazon Cost Explorer Service 的条件键

Amazon Cost Explorer 服务定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString

Amazon Data Lifecycle Manager 的操作、资源和条件键

Amazon Data Lifecycle Manager（服务前缀：dlm）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Data Lifecycle Manager 定义的操作

- Amazon Data Lifecycle Manager 定义的资源类型
- Amazon Data Lifecycle Manager 的条件键

Amazon Data Lifecycle Manager 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateLifecyclePolicy	授予权限以创建数据生命周期策略来管理计划的 Amazon EBS 快照创建和保留。您最多可以具有 100 个策略	写入		aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteLifecyclePolicy	授予权限以删除现有的数据生命周期策略。此外，该操作还会停止创建和删除策略指定的快照。现有快照不受影响	写入	policy*		
GetLifecyclePolicies	授予权限以返回数据生命周期策略的摘要描述列表	列表			
GetLifecyclePolicy	授予权限以返回单个数据生命周期策略的完整描述	读取	policy*		
ListTagsForResource	授予权限以列出与资源关联的标签	读取	policy*		
TagResource	授予权限以添加或更新资源的标签	标记	policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予权限以删除与资源关联的标签	标记	policy*		
				aws:TagKeys	
UpdateLifecyclePolicy	授予权限以更新现有的数据生命周期策略	写入	policy*		

Amazon Data Lifecycle Manager 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从

而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
policy	arn:${Partition}:dlm:${Region}:${Account}:policy/${ResourceName}	aws:ResourceTag/${TagKey}

Amazon Data Lifecycle Manager 的条件键

Amazon Data Lifecycle Manager 定义以下可以在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按附加到资源的标签键值对筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString

Amazon Database Migration Service 的操作、资源和条件键

Amazon Database Migration Service（服务前缀:dms）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon Database Migration Service 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddTagsToResource	授予向 DMS 资源（包括复制实例、终端节点、安全组和迁	Tagging	Certificate		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
	移任务）添加元数据标签的权限		DataMigration		
			DataProvider		
			Endpoint		
			EventSubscription		
			InstanceProfile		
			MigrationProject		
			ReplicationConfig		
			ReplicationInstance		
			ReplicationSubnetGroup		
			ReplicationTask		
			ReplicationTaskAssessmentRun		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			ReplicationTaskIndividualAssessment		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
ApplyPendingMaintenanceAction	授予将待处理的维护操作应用于资源（例如，应用于复制实例）的权限	写入	ReplicationInstance*		
AssociateExtensionPack	授予权限以关联扩展包	写入	MigrationProject*		dms:StartExtensionPackAssociation
BatchStartRecommendations	授予权限以开始分析最多 20 个源数据库，从而为每个源数据库推荐目标引擎	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CancelMetadataModelAssessment	授予权限以取消单个元数据模型评估运行	写入	MigrationProject*		
CancelMetadataModelConversion	授予权限以取消单个元数据模型转换运行	写入	MigrationProject*		
CancelMetadataModelExport	授予权限以取消单个元数据模型导出运行	写入	MigrationProject*		
CancelReplicationTaskAssessmentRun	授予取消单个迁移前评估运行的权限	写入	ReplicationTaskAssessmentRun*		
CreateDataMigration	授予使用提供的设置创建数据库迁移的权限	写入	MigrationProject*		iam:PassRole
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateDataProvider	授予权限以使用提供的设置创建数据提供程序	写入		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole
CreateEndpoint	授予使用提供的设置创建终端节点的权限	写入		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateEventSubscription	授予创建 Amazon DMS 事件通知订阅的权限	写入		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
CreateFleetAdvisorCollector	授予使用指定参数创建 Fleet Advisor 收集器的权限	写入			iam:PassRole
CreateInstanceProfile	授予权限以使用提供的设置创建实例配置文件	写入		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateMigrationProject	授予权限以使用提供的设置创建迁移项目	写入	DataProvider*		iam:PassRole
			InstanceProfile*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
CreateReplicationConfig	授予使用提供的设置创建复制配置的权限	写入	Endpoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
CreateReplicationInstance	授予使用指定参数创建复制实例的权限	写入		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateReplicationSubnetGroup	根据 VPC 中的子网列表，授予创建复制子网组 IDs 的权限	写入		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
CreateReplicationTask	授予使用指定参数创建复制任务的权限	Write	Endpoint* ReplicationInstance*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
DeleteCertificate	授予删除指定证书的权限	Write	Certificate*		
DeleteConnection	授予删除复制实例和终端节点之间的指定连接的权限	写入	Endpoint* ReplicationInstance*		
DeleteDataMigration	授予删除指定的数据库迁移的权限	写入	DataMigration*		
DeleteDataProvider	授予权限以删除指定的数据提供程序	写入	DataProvider*		
DeleteEndpoint	授予删除指定终端节点的权限	写入	Endpoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteEventSubscription	授予删除 Amazon DMS 活动订阅的权限	写入	EventSubscription*		
DeleteFleetAdvisorCollector	授予删除指定 Fleet Advisor 收集器的权限	写入			
DeleteFleetAdvisorDatabases	授予删除指定 Fleet Advisor 数据库的权限	写入			
DeleteInstanceProfile	授予权限以删除指定的实例配置文件	写入	InstanceProfile*		
DeleteMigrationProject	授予权限以删除指定的迁移项目	写入	MigrationProject*		
DeleteReplicationConfig	授予删除指定的复制配置的权限	写入	ReplicationConfig*		
DeleteReplicationInstance	授予删除指定复制实例的权限	Write	ReplicationInstance*		
DeleteReplicationSubnetGroup	授予删除子网组的权限	Write	ReplicationSubnetGroup*		
DeleteReplicationTask	授予删除指定复制任务的权限	Write	ReplicationTask*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteReplicationTaskAssessmentRun	授予删除单个迁移前评估运行记录的权限	写入	ReplicationTaskAssessmentRun*		
DescribeAccountAttributes	授予列出客户账户所有 Amazon DMS 属性的权限	读取			
DescribeApplicableIndividualAssessments	授予列出可为新迁移前评估运行指定的单个评估的权限	Read	ReplicationInstance		
			ReplicationTask		
DescribeCertificates	授予提供证书描述的权限	Read			
DescribeConnections	授予描述在复制实例与终端节点之间已建立的连接状态的权限	读取			
DescribeConversionConfiguration	授予返回有关 DMS 架构转换项目配置信息的权限	读取	MigrationProject*		
DescribeDataMigrations	授予返回指定区域中您账户的数据库迁移信息的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeDataProviders[仅权限]	授予列出数据提供者的 Amazon DMS 属性的权限。注意。此操作应与上述架构转换操作一起添加 ListDataProviders，但目前并未授权该操作	读取	DataProvider		dms:ListDataProviders
DescribeEndpointSettings	授予在为特定数据库引擎创建终端节点时返回可能的终端节点设置的权限	读取			
DescribeEndpointTypes	授予返回有关可用终端节点类型的信息的权限	Read			
DescribeEndpoints	授予返回有关当前区域账户终端节点信息的权限	读取			
DescribeEngineVersions	授予权限以返回 DMS 复制实例可用版本的相关信息	读取			
DescribeEventCategories	授予列出所有事件源类型的类别（或如果指定，则列出指定源类型的类别）的权限	Read			
DescribeEventSubscriptions	授予列出客户账户的所有订阅描述的权限	Read			
DescribeEvents	授予列出给定源标识符和源类型事件的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeExtensionPackAssociations[仅权限]	授予列出扩展包的 Amazon DMS 属性的权限。注意。此操作应与上述架构转换操作一起添加 ListExtensionPacks，但目前并未授权该操作	读取	MigrationProject*		dms:ListExtensionPacks
DescribeFleetAdvisorCollectors	授予根据筛选条件设置返回账户中 Fleet Advisor 收集器分页列表的权限	读取			
DescribeFleetAdvisorDatabases	授予根据筛选条件设置返回账户中 Fleet Advisor 数据库分页列表的权限	读取			
DescribeFleetAdvisorLsaAnalysis	授予返回由 Fleet Advisor 收集器生成的大规模评估 (LSA) 分析描述的分页列表的权限	读取			
DescribeFleetAdvisorSchemaObjectSummary	授予返回 Fleet Advisor 收集器根据筛选条件设置发现的架构描述的分页列表的权限	读取			
DescribeFleetAdvisorSchemas	授予返回 Fleet Advisor 收集器根据筛选条件设置发现的架构分页列表的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeInstanceProfiles[仅权限]	授予列出实例配置文件的 Amazon DMS 属性的权限。注意。此操作应与上述架构转换操作一起添加 ListInstanceProfiles，但目前并未授权该操作	读取	InstanceProfile		dms:ListInstanceProfiles
DescribeMetadataModelAssessments[仅权限]	授予列出元数据模型评估的 Amazon DMS 属性的权限。注意。此操作应与上述架构转换操作一起添加 ListMetadataModelAssessments，但目前并未授权该操作	读取	MigrationProject*		dms:ListMetadataModelAssessments
DescribeMetadataModelConversions[仅权限]	授予列出元数据模型转换的 Amazon DMS 属性的权限。注意。此操作应与上述架构转换操作一起添加 ListMetadataModelConversions，但目前并未授权该操作	读取	MigrationProject*		dms:ListMetadataModelConversions
DescribeMetadataModelExportsAsScript[仅权限]	授予列出元数据模型导出的 Amazon DMS 属性的权限。注意。此操作应与上述架构转换操作一起添加 ListMetadataModelExports，但目前并未授权该操作	读取	MigrationProject*		dms:ListMetadataModelExports

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeMetadataModelExportsToTarget[仅权限]	授予列出元数据模型导出的 Amazon DMS 属性的权限。注意。此操作应与上述架构转换操作一起添加 ListMetadataModelExports，但目前并未授权该操作	读取	MigrationProject*		dms:ListMetadataModelExports
DescribeMetadataModelImports	授予返回有关启动迁移项目元数据模型导入操作信息的权限	读取	MigrationProject*		
DescribeMigrationProjects[仅权限]	授予列出迁移项目的 Amazon DMS 属性的权限。注意。此操作应与上述架构转换操作一起添加 ListMigrationProjects，但目前并未授权该操作	读取	DataProvider		dms:ListMigrationProjects
			InstanceProfile		
			MigrationProject		
DescribeOrderableReplicationInstances	授予返回有关可在指定区域内创建的复制实例类型信息的权限	读取			
DescribePendingMaintenanceActions	授予返回待处理维护操作相关信息的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeRecommendationLimitations	授予返回目标 Amazon 引擎推荐限制的分页列表的权限	读取			
DescribeRecommendations	授予权限以返回源数据库的目标引擎推荐说明的分页列表	读取			
DescribeRefreshSchemasStatus	授予返回 RefreshSchemas 操作状态的权限	读取	Endpoint*		
DescribeReplicationConfigs	授予描述复制配置的权限	读取			
DescribeReplicationInstanceTaskLogs	授予返回有关指定任务的任务日志信息的权限	Read	ReplicationInstance*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
DescribeReplicationInstances	授予返回有关当前区域中账户的复制实例信息的权限	Read			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeReplicationSubnetGroups	授予返回有关复制子网组信息的权限	读取			
DescribeReplicationTableStatistics	授予描述复制表统计信息的权限	读取	ReplicationConfig*		
DescribeReplicationTaskAssessmentResults	授予从 Amazon S3 返回最新任务评估结果的权限	Read	ReplicationTask		
DescribeReplicationTaskAssessmentRuns	授予根据过滤器设置返回迁移前评估运行的分页列表的权限	Read	ReplicationInstance		
			ReplicationTask		
			ReplicationTaskAssessmentRun		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeReplicationTaskIndividualAssessments	授予根据筛选条件设置返回单个评估的分页列表的权限	Read	ReplicationTask		
			ReplicationTaskAssessmentRun		
DescribeReplicationTasks	授予返回有关您账户在当前区域的复制任务信息的权限	读取			
DescribeReplications	授予描述复制的权限	读取			
DescribeSchemas	授予返回有关指定终端节点的架构信息的权限	Read	Endpoint*		
DescribeTableStatistics	授予返回有关数据库迁移任务的表统计数据（包括表名称、插入的行、更新的行和删除的行）的权限	读取	ReplicationTask*		
DisassociateExtensionPack	授予权限以取消关联扩展包	写入	MigrationProject*		
ExportMetadataModelAssessment	授予权限以导出指定的元数据模型评估	写入	MigrationProject		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetMetadataModel	授予列出元数据模型所有 Amazon DMS 属性的权限。注意。尽管需要执行此操作 StartMetadataModelImport，但后者目前并未授权上述架构转换操作	读取	MigrationProject		dms:StartMetadataModelImport
ImportCertificate	授予上传指定证书的权限	写入		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
ListDataProviders	授予列出数据提供者的 Amazon DMS 属性的权限	读取	DataProvider		dms:DescribeDataProviders
ListExtensionPacks	授予列出扩展 Amazon 包的 DMS 属性的权限	读取	MigrationProject		dms:DescribeExtensionPackAssociations
ListInstanceProfiles	授予列出实例配置 Amazon 文件的 DMS 属性的权限	读取	InstanceProfile		dms:DescribeInstanceProfiles

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListMetadataModelAssessmentActionItems	授予列出元数据模型评估措施项的 Amazon DMS 属性的权限。注意。尽管需要执行此操作 StartMetadataModelImport，但后者目前并未授权上述架构转换操作	读取	MigrationProject		dms:StartMetadataModelImport
ListMetadataModelAssessments	授予列出元数据模型评估的 Amazon DMS 属性的权限	读取	MigrationProject		dms:DescribeMetadataModelAssessments
ListMetadataModelConversions	授予列出元数据模型转换的 Amazon DMS 属性的权限	读取	MigrationProject		dms:DescribeMetadataModelConversions
ListMetadataModelExports	授予列出元数据模型导出的 Amazon DMS 属性的权限	读取	MigrationProject		dms:DescribeMetadataModelExportsAsScript dms:DescribeMetadataModelExportsToTarget

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListMigrationProjects	授予列出迁移项目的 Amazon DMS 属性的权限。注意。尽管此操作需要 DescribeMigrationProjects 和 DescribeConversionConfiguration，但这两个必需的操作目前都未授权上述架构转换操作	读取	DataProvider		dms:DescribeConversionConfiguration dms:DescribeMigrationProjects
			InstanceProfile		
			MigrationProject		
ListTagsForResource	授予列出 Amazon DMS 资源所有标签的权限	读取	Certificate		
			DataMigration		
			DataProvider		
			Endpoint		
			EventSubscription		
			InstanceProfile		
			MigrationProject		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			ReplicationConfig		
			ReplicationInstance		
			ReplicationSubnetGroup		
			ReplicationTask		
			ReplicationTaskAssessmentRun		
			ReplicationTaskIndividualAssessment		
ModifyConversionConfiguration[仅权限]	授予更新转换配置的权限。注意。此操作应与上述架构转换操作一起添加 UpdateConversionConfiguration，但目前并未授权该操作	写入	MigrationProject*		dms:UpdateConversionConfiguration
ModifyDataMigration	授予修改指定的数据库迁移的权限	写入	DataMigration*		iam:PassRole

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ModifyDataProvider[仅权限]	授予修改指定数据提供程序的权限。注意。此操作应与上述架构转换操作一起添加 UpdateDataProvider，但目前并未授权该操作	写入	DataProvider*		dms:UpdateDataProvider iam:PassRole
ModifyEndpoint	授予权限以修改指定端点	写入	Endpoint*		iam:PassRole
			Certificate		
ModifyEventSubscription	授予修改现有 Amazon DMS 事件通知订阅的权限	写入			
ModifyFleetAdvisorCollector[仅权限]	授予修改指定 Fleet Advisor 收集器的名称和描述的权限	写入			
ModifyFleetAdvisorCollectorStatuses[仅权限]	授予修改指定 Fleet Advisor 收集器状态的权限	写入			
ModifyInstanceProfile[仅权限]	授予修改指定实例配置文件的权限。注意。此操作应与上述架构转换操作一起添加 UpdateInstanceProfile，但目前并未授权该操作	写入	InstanceProfile*		dms:UpdateInstanceProfile iam:PassRole

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ModifyMigrationProject[仅权限]	授予修改指定迁移项目的权限。注意。此操作应与上述架构转换操作一起添加 UpdateMigrationProject，但目前并未授权该操作	写入	MigrationProject*		dms:UpdateMigrationProject iam:PassRole
ModifyReplicationConfig	授予修改指定的复制配置的权限	写入	ReplicationConfig*		
ModifyReplicationInstance	授予修改复制实例以应用新设置的权限	Write	ReplicationInstance*		
ModifyReplicationSubnetGroup	授予修改指定复制子网组设置的权限	Write			
ModifyReplicationTask	授予修改指定复制任务的权限	Write	ReplicationTask*		
MoveReplicationTask	授予将指定复制任务移动到其他复制实例的权限	Write	ReplicationInstance* ReplicationTask*		
RebootReplicationInstance	授予重启复制实例的权限。重启将导致暂时中断，直到复制实例再次变为可用	Write	ReplicationInstance*		
RefreshSchemas	授予为指定终端节点填充架构的权限	写入	Endpoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			ReplicationInstance*		
ReloadReplicationTables	授予使用复制源重新加载目标数据库表的权限	写入	ReplicationConfig*		
ReloadTables	授予使用源数据重新加载目标数据库表的权限	Write	ReplicationTask*		
RemoveTagsFromResource	授予从 DMS 资源中删除元数据标签的权限	标记	Certificate		
			DataMigration		
			DataProvider		
			Endpoint		
			EventSubscription		
			InstanceProfile		
			MigrationProject		
			ReplicationConfig		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			ReplicationInstance		
			ReplicationSubnetGroup		
			ReplicationTask		
			ReplicationTaskAssessmentRun		
			ReplicationTaskIndividualAssessment		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
RunFleetAdvisorLsaAnalysis	授予对账户中的每个 Fleet Advisor 收集器进行大规模评估 (LSA) 分析的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StartDataMigration	授予启动数据库迁移的权限	写入	DataMigration*		
StartExtensionPackAssociation[仅权限]	授予关联扩展包的权限。注意。此操作应与上述架构转换操作一起添加 AssociateExtensionPack，但目前并未授权该操作	写入	MigrationProject*		dms:AssociateExtensionPack
StartMetadataModelAssessment	授予权限以启动元数据模型的新评估	写入	MigrationProject*		
StartMetadataModelConversion	授予权限以启动元数据模型的新转换	写入	MigrationProject*		
StartMetadataModelExportAsScript[仅权限]	授予以脚本形式启动元数据模型新导出的权限。注意。此操作应与上述架构转换操作一起添加 StartMetadataModelExportAsScripts，但目前并未授权该操作	写入	MigrationProject*		dms:StartMetadataModelExportAsScripts
StartMetadataModelExportAsScripts	授予权限以将元数据模型的新导出作为脚本启动	写入	MigrationProject*		dms:StartMetadataModelExportAsScript
StartMetadataModelExportToTarget	授予权限以将元数据模型的新导出启动到目标	写入	MigrationProject*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StartMetadataModelImport	授予权限以启动元数据模型的新导入	写入	MigrationProject*		
StartRecommendations	授予权限以启动对源数据库的分析，从而提供目标引擎的建议	写入			
StartReplication	授予启动复制的权限	写入	ReplicationConfig*		
StartReplicationTask	授予启动复制任务的权限	Write	ReplicationTask*		
StartReplicationTaskAssessment	授予为源数据库中的不支持的数据类型启动复制任务评估的权限	Write	ReplicationTask*		
StartReplicationTaskAssessmentRun	授予为迁移任务的一个或多个单独评估启动新的迁移前评估运行的权限	写入	ReplicationTask*		iam:PassRole
StopDataMigration	授予停止数据库迁移的权限	写入	DataMigration*		
StopReplication	授予停止复制的权限	写入	ReplicationConfig*		
StopReplicationTask	授予停止复制任务的权限	Write	ReplicationTask*		
TestConnection	授予测试复制实例和终端节点之间连接的权限	读取	Endpoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			ReplicationInstance*		
UpdateConversionConfiguration	授予权限以更新转换配置	写入	MigrationProject*		dms:ModifyConversionConfiguration
UpdateDataProvider	授予权限以更新指定的数据提供程序	写入	DataProvider*		dms:ModifyDataProvider
UpdateInstanceProfile	授予权限以更新指定的实例配置文件	写入	InstanceProfile*		dms:ModifyInstanceProfile
UpdateMigrationProject	授予权限以更新指定的迁移项目	写入	MigrationProject*		dms:ModifyMigrationProject
UpdateSubscriptionsToEventBridge	授予将 DMS 订阅迁移到 Eventbridge 的权限	写入			
UploadFileMetadataList[仅权限]	授予将文件上传到 Amazon S3 桶的权限	写入			

Amazon Database Migration Service 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从

而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
Certificate	arn:${Partition}:dms:${Region}:${Account}:cert:*	aws:ResourceTag/${TagKey} dms:cert-tag/${TagKey}
DataProvider	arn:${Partition}:dms:${Region}:${Account}:data-provider:*	aws:ResourceTag/${TagKey} dms:data-provider-tag/${TagKey}
DataMigration	arn:${Partition}:dms:${Region}:${Account}:data-migration:*	aws:ResourceTag/${TagKey} dms:data-migration-tag/${TagKey}
Endpoint	arn:${Partition}:dms:${Region}:${Account}:endpoint:*	aws:ResourceTag/${TagKey} dms:endpoint-tag/${TagKey}
EventSubscription	arn:${Partition}:dms:${Region}:${Account}:es:*	aws:ResourceTag/${TagKey} dms:es-tag/${TagKey}
InstanceProfile	arn:${Partition}:dms:${Region}:${Account}:instance-profile:*	aws:ResourceTag/${TagKey} dms:instance-profile-tag/${TagKey}

资源类型	ARN	条件键
MigrationProject	arn:${Partition}:dms:${Region}:${Account}:migration-project:*	aws:ResourceTag/${TagKey} dms:migration-project-tag/${TagKey}
ReplicationConfig	arn:${Partition}:dms:${Region}:${Account}:replication-config:*	aws:ResourceTag/${TagKey} dms:replication-config-tag/${TagKey}
ReplicationInstance	arn:${Partition}:dms:${Region}:${Account}:rep:*	aws:ResourceTag/${TagKey} dms:rep-tag/${TagKey}
ReplicationSubnetGroup	arn:${Partition}:dms:${Region}:${Account}:subgrp:*	aws:ResourceTag/${TagKey} dms:subgrp-tag/${TagKey}
ReplicationTask	arn:${Partition}:dms:${Region}:${Account}:task:*	aws:ResourceTag/${TagKey} dms:task-tag/${TagKey}
ReplicationTaskAssessmentRun	arn:${Partition}:dms:${Region}:${Account}:assessment-run:*	aws:ResourceTag/${TagKey} dms:assessment-run-tag/${TagKey}

资源类型	ARN	条件键
ReplicationTaskIndividualAssessment	arn:${Partition}:dms:${Region}:${Account}:individual-assessment:*	aws:ResourceTag/${TagKey} dms:individual-assessment-tag/${TagKey}

Amazon Database Migration Service 的条件键

Amazon Database Migration Service 定义了以下可用于 IAM 策略Condition元素的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对来筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按是否存在附加到资源的标签键值对筛选访问权限	字符串
aws:TagKeys	根据在请求中是否具有标签键来筛选访问	ArrayOfString
dms:assessment-run-tag/${TagKey}	根据请求中是否存在标签键值对来筛选访问权限 AssessmentRun	字符串
dms:cert-tag/${TagKey}	根据在 Certificate 请求中是否具有标签键值对来筛选访问权限	字符串
dms:data-migration-tag/${TagKey}	根据请求中是否存在标签键值对来筛选访问权限 DataMigration	字符串

条件键	描述	类型
dms:data-provider-tag/${TagKey}	根据请求中是否存在标签键值对来筛选访问权限 DataProvider	字符串
dms:endpoint-tag/${TagKey}	根据在 Endpoint 请求中是否具有标签键值对来筛选访问权限	字符串
dms:es-tag/${TagKey}	根据请求中是否存在标签键值对来筛选访问权限 EventSubscription	字符串
dms:individual-assessment-tag/${TagKey}	根据请求中是否存在标签键值对来筛选访问权限 IndividualAssessment	字符串
dms:instance-profile-tag/${TagKey}	根据请求中是否存在标签键值对来筛选访问权限 InstanceProfile	字符串
dms:migration-project-tag/${TagKey}	根据请求中是否存在标签键值对来筛选访问权限 MigrationProject	字符串
dms:rep-tag/${TagKey}	根据请求中是否存在标签键值对来筛选访问权限 ReplicationInstance	字符串
dms:replication-config-tag/${TagKey}	根据请求中是否存在标签键值对来筛选访问权限 ReplicationConfig	字符串
dms:req-tag/${TagKey}	根据在给定请求中是否具有标签键值对来筛选访问权限	字符串
dms:subgrp-tag/${TagKey}	根据请求中是否存在标签键值对来筛选访问权限 ReplicationSubnetGroup	字符串
dms:task-tag/${TagKey}	根据请求中是否存在标签键值对来筛选访问权限 ReplicationTask	字符串

Amazon Direct Connect 的操作、资源和条件键

Amazon Direct Connect（服务前缀:directconnect）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon Direct Connect 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AcceptDirectConnectGatewayAssociationProposal	授予权限以接受提议请求以将虚拟私有网关连接到 Direct Connect 网关	写入	dx-gateway*		
AllocateConnectionOnInterconnect	授予权限以在互连上创建托管连接	写入	dxcon*		
AllocateHostedConnection	授予在 Di Amazon rect Connect 合作伙伴的网络和特定 Amazon 的 Direct Connect 位置之间创建新的托管连接的权限	写入	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
AllocatePrivateVirtualInterface	授予权限以预置将由不同客户拥有的私有虚拟接口	写入	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AllocatePublicVirtualInterface	授予权限以预置将由不同客户拥有的公有虚拟接口	写入	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
AllocateTransitVirtualInterface	授予权限以预置将由不同客户拥有的中转虚拟接口	写入	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
AssociateConnectionWithLag	授予将连接与 LAG 关联的权限	写入	dxcon*		
			dxlag*		
AssociateHostedConnection	授予权限以将托管的连接及其虚拟接口与链路聚合组 (LAG) 或互连相关联	写入	dxcon*		
			dxcon		
			dxlag		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateMacSecKey	授予将 MAC 安全 (MACsec) 连接密钥名称 (CKN) /连接关联密钥 (CAK) 对与 Di Amazon rect Connect 专用连接关联的权限	写入	dxcon		
			dxlag		
AssociateVirtualInterface	授予权限以将虚拟接口与指定的链路聚合组 (LAG) 或连接相关联	写入	dxvif*		
			dxcon		
			dxlag		
ConfirmConnection	授予权限以确认在互连上创建托管连接	写入	dxcon*		
ConfirmCustomerAgreement	授予权限以在创建连接或链路聚合组 (LAG) 时确认协议条款	写入			
ConfirmPrivateVirtualInterface	授予权限以接受其他客户创建的私有虚拟接口的所有权	写入	dxvif*		
ConfirmPublicVirtualInterface	授予权限以接受其他客户创建的公有虚拟接口的所有权	写入	dxvif*		
ConfirmTransitVirtualInterface	授予权限以接受其他客户创建的中转虚拟接口的所有权	写入	dxvif*		
CreateBGPPeer	授予权限以在指定的虚拟接口上创建 BGP 对等体	写入	dxvif*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateConnection	授予在客户网络和特定的 Di Amazon rect Connect 位置之间创建新连接的权限	写入	dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDirectConnectGateway	授予权限以创建一个 Direct Connect 网关，它是可用于连接一组虚拟接口和虚拟专用网关的中间对象	写入			
CreateDirectConnectGatewayAssociation	授予权限以在 Direct Connect 网关和虚拟私有网关之间创建关联	写入	dx-gateway*		
CreateDirectConnectGatewayAssociationProposal	授予创建提议以将指定的虚拟私有网关与指定的 Direct Connect 网关相关联的权限	写入	dx-gateway*		
CreateInterconnect	授予在 Direct Connect 合作伙伴的网络和特定 Amazon 的 Di Amazon rect Connect 位置之间创建新互连的权限	写入	dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateLag	授予在客户网络和特定 Dire Amazon ct Connect 位置之间使用指定数量的捆绑物理连接创建链路聚合组 (LAG) 的权限	写入	dxcon		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePrivateVirtualInterface	授予权限以创建新的私有虚拟接口	写入	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePublicVirtualInterface	授予权限以创建新的公有虚拟接口	写入	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTransitVirtualInterface	授予权限以创建新的中转虚拟接口	写入	dxcon		
			dxlag		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBGPPeer	授予权限以删除具有指定客户地址和 ASN 的指定虚拟接口上的指定 BGP 对等体	写入	dxvif*		
DeleteConnection	授予权限以删除连接	写入	dxcon*		
DeleteDirectConnectGateway	授予删除指定 Direct Connect 网关的权限	写入	dx-gateway*		
DeleteDirectConnectGatewayAssociation	授予权限以删除指定的 Direct Connect 网关和虚拟私有网关之间的关联	写入	dx-gateway*		
DeleteDirectConnectGatewayAssociationProposal	授予权限以删除指定的 Direct Connect 网关和虚拟私有网关之间的关联提议请求	写入			
DeleteInterconnect	授予删除指定互连的权限	写入	dxcon*		
DeleteLag	授予删除指定的链接聚合组 (LAG) 的权限	写入	dxlag*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteVirtualInterface	授予删除虚拟接口的权限	写入	dxvif*		
DescribeConnectionLoa	授予权限以描述连接的 LOA-CFA	读取	dxcon*		
DescribeConnections	授予权限以描述此区域中的所有连接	读取	dxcon		
DescribeConnectionsOnInterconnect	授予权限以描述给定互连中已预置的连接的列表。	读取	dxcon*		
DescribeCustomerMetadata	授予查看客户协议列表的权限，以及其签署状态以及客户是 NNIPartner V2 还是非合作伙伴 NNIPartner	读取			
DescribeDirectConnectGatewayAssociationProposals	授予权限以描述虚拟私有网关和 Direct Connect 网关之间的连接的一个或多个关联提议。	读取	dx-gateway		
DescribeDirectConnectGatewayAssociations	授予权限以描述 Direct Connect 网关和虚拟私有网关之间的关联	读取	dx-gateway		
DescribeDirectConnectGatewayAttachments	授予权限以描述 Direct Connect 网关和虚拟接口之间的连接	读取	dx-gateway		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeDirectConnectGateways	授予权限以描述所有 Direct Connect 网关，或仅描述指定的 Direct Connect 网关	读取	dx-gateway		
DescribeHostedConnections	授予权限以描述已在指定互连或链路聚合组上预置的托管连接	读取	dxcon		
			dxlag		
DescribeInterconnectLoa	授予权限以描述互连的 LOA-CFA	读取	dxcon*		
DescribeInterconnects	授予描述所拥有的互连列表的权限 Amazon Web Services 账户	读取	dxcon		
DescribeLags	授予权限以描述所有的链接聚合组 (LAG) 或指定的 LAG	读取	dxlag		
DescribeLoa	授予权限以描述连接、互连或链路聚合组 (LAG) 的 LOA-CFA	读取	dxcon		
			dxlag		
DescribeLocations	授予描述当前 Amazon 区域中 Di Amazon rect Connect 位置列表的权限	读取			
DescribeRouterConfiguration	授予权限以描述虚拟接口路由器的详细信息	读取	dxvif*		
DescribeTags	授予描述与指定 Di Amazon rect Connect 资源关联的标签的权限	读取	dxcon		
			dxlag		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			dxvif		
DescribeVirtualGateways	授予描述拥有的虚拟专用网关列表的权限 Amazon Web Services 账户	读取			
DescribeVirtualInterfaces	授予描述所有虚拟接口的权限 Amazon Web Services 账户	读取	dxcon		
			dxlag		
			dxvif		
DisassociateConnectionFromLag	授予权限以取消连接与链路聚合组 (LAG) 的关联	写入	dxcon*		
			dxlag*		
DisassociateMacSecKey	授予移除 MAC 安全 (MACsec) 安全密钥和 Di Amazon rect Connect 专用连接之间关联的权限	写入	dxcon		
			dxlag		
ListVirtualInterfaceTestHistory	授予权限以列出虚拟接口故障转移测试历史记录	列表	dxvif*		
StartBgpFailoverTest	授予权限以启动虚拟接口故障转移测试，此测试通过将 BGP 对等会话置于“关闭”状态，验证您的配置是否符合弹性要求。然后，您可以发送流量以便验证是否出现中断情况	写入	dxvif*		
StopBgpFailoverTest	授予权限以停止虚拟接口故障转移测试	写入	dxvif*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
TagResource	授予向指定的 Di Amazon rect Connect 资源添加指定标签的权限。每个资源最多可以有 50 个标签	标记	dxcon		
			dxlag		
			dxvif		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予从指定的 Di Amazon rect Connect 资源中移除一个或多个标签的权限	标记	dxcon		
			dxlag		
			dxvif		
				aws:TagKeys	
UpdateConnection	授予更新 Di Amazon rect Connect 专用连接配置的权限。您可以更新连接的以下参数：连接名称或连接的 MAC Security (MACsec) 加密模式	写入	dxcon*		
UpdateDirectConnectGateway	授予权限以更新 Direct Connect 网关的名称	写入	dx-gateway*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateDirectConnectGatewayAssociation	授予权限以更新 Direct Connect 网关关联的指定属性	写入			
UpdateLag	授予权限以更新指定链路聚合组 (LAG) 的属性	写入	dxlag*		
UpdateVirtualInterfaceAttributes	授予权限以更新指定虚拟私有接口的指定属性	写入	dxvif*		

Amazon Direct Connect 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
dxcon	`arn:${Partition}:directconnect:${Region}:${Account}:dxcon/${ConnectionId}`	aws:ResourceTag/${TagKey}
dxlag	`arn:${Partition}:directconnect:${Region}:${Account}:dxlag/${LagId}`	aws:ResourceTag/${TagKey}
dxvif	`arn:${Partition}:directconnect:${Region}:${Account}:dxvif/${VirtualInterfaceId}`	aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
dx-gateway	arn:${Partition}:directconnect::${Account}:dx-gateway/${DirectConnectGatewayId}	

Amazon Direct Connect 的条件键

Amazon Direct Connect 定义了以下可以在 IAM 策略Condition元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对来按照操作筛选访问权限	字符串
aws:ResourceTag/${TagKey}	根据附加到资源的标签键值对来按操作筛选访问权限	字符串
aws:TagKeys	根据在请求中是否具有标签键来按操作筛选访问权限	ArrayOfString

Amazon Directory Service 的操作、资源和条件键

Amazon Directory Service（服务前缀:ds）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Directory Service 定义的操作

- Amazon Directory Service 定义的资源类型
- Amazon Directory Service 的条件键

Amazon Directory Service 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AcceptSharedDirectory	授予接受从目录所有者账户中发送的目录共享请求的权限	写入	directory*		
AccessDSData[仅权限]	授予权限以使用 Directory Service Data API 访问目录数据	权限管理	directory*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddIpRoutes	授予添加 CIDR地址块以便在 Amazon Web Services 上的 Microsoft AD 之间正确路由流量的权限	写入	directory*		ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:DescribeSecurityGroups

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddRegion	授予在指定目录的指定区域中添加两个域控制器的权限	写入	directory*		ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddTagsToResource	授予为指定的 Amazon Directory Services 目录添加或覆盖一个或多个标签的权限	标记	directory*		ec2:CreateTags
				aws:RequestTag/${TagKey} aws:TagKeys	
AuthorizeApplication[仅权限]	授予授权您的 Amazon 目录应用程序的权限	写入	directory*		
CancelSchemaExtension	授予取消至 Microsoft AD 目录的正在进行的架构扩展的权限	写入	directory*		
CheckAlias[仅权限]	授予验证别名是否可供使用的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ConnectDirectory	授予创建 AD Connector 以连接到本地目录的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
CreateAlias	授予为目录创建别名并将别名分配至目录的权限	写入	directory*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateComputer	授予在指定目录中创建计算机帐户并将该计算机加入该目录的权限	写入	directory*		
CreateConditionalForwarder	授予创建与您的 Amazon 目录关联的条件转发器的权限	写入	directory*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateDirectory	授予创建 Simple AD 目录的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateIdentityPoolDirectory[仅权限]	授予在 Amazon 云中创建 IdentityPool 目录的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLogSubscription	授予创建订阅的权限，以便将实时 Directory Service 域控制器安全 CloudWatch 日志转发到您的指定日志组 Amazon Web Services 账户	写入	directory*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateMicrosoftAD	授予在 Amazon 云端创建 Microsoft 广告的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateSnapshot	授予在 Amazon 云中创建 Simple AD 或 Microsoft AD 目录快照的权限	写入	directory*		
CreateTrust	授予权限以启动在 Amazon 云 Amazon 端的 Microsoft AD 与外部域之间建立信任关系的侧面	写入	directory*		
DeleteConditionalForwarder	授予删除已为您的 Amazon 目录设置的条件转发器的权限	写入	directory*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteDirectory	授予删除 D Amazon irectory Service 目录的权限	写入	directory*		ec2:DeleteNetworkInterface ec2:DeleteSecurityGroup ec2:DescribeNetworkInterfaces ec2:RevokeSecurityGroupEgress ec2:RevokeSecurityGroupIngress
DeleteLogSubscription	授予删除指定日志订阅的权限	写入	directory*		
DeleteSnapshot	授予删除目录快照的权限	写入	directory*		
DeleteTrust	授予删除 Amazon 云中你的 Microsoft AD 与外部域之间现有信任关系的权限	写入	directory*		
DeregisterCertificate	授予从系统中删除在安全的 DAP 连接中注册的证书的权限	写入	directory*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeregisterEventTopic	授予以发布商身份删除至指定 SNS 主题的指定目录的权限	写入	directory*		
DescribeCertificate	授予显示在安全的 LDAP 连接中注册的证书相关信息的权限	读取	directory*		
DescribeClientAuthenticationSettings	授予检索指定目录（如已指定）中的客户端身份验证类型相关信息的权限。如未指定类型，则会检索与指定目录支持的所有客户端身份验证类型相关的信息。当前，SmartCard 仅支持	读取	directory*		
DescribeConditionalForwarders	授予获取此账户的条件转发服务器相关信息的权限	读取	directory*		
DescribeDirectories	授予获取属于此账户的目录相关信息的权限	列表			
DescribeDirectoryDataAccess	授予权限以描述指定目录的 Directory Service Data API 状态	读取	directory*		
DescribeDomainControllers	授予提供有关目录中的任何域控制器信息的权限	读取	directory*		
DescribeEventTopics	授予获取哪些 SNS 主题从指定目录接收状态消息相关信息的权限	读取	directory*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeLDAPSSettings	授予描述指定目录的 LDAP 安全性状态的权限	读取	directory*		
DescribeRegions	授予提供为多区域复制配置的区域相关信息的权限	读取	directory*		
DescribeSettings	授予检索有关指定目录可配置设置的信息的权限	读取	directory*		
DescribeSharedDirectories	授予返回账户中的共享目录的权限	读取	directory*		
DescribeSnapshots	授予获取属于此账户的目录快照相关信息的权限	读取			
DescribeTrusts	授予获取此账户的信任关系的相关信息的权限	读取			
DescribeUpdateDirectory	授予权限以描述特定更新类型的目录更新	读取	directory*		
DisableClientAuthentication	授予禁用指定目录的替代客户端身份验证方法的权限	写入	directory*		
DisableDirectoryDataAccess	授予权限以禁用指定目录的 Directory Service Data API	写入	directory*		
DisableLDAPS	授予停用指定目录的 LDAP 安全调用的权限	写入	directory*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DisableRadius	授予针对 AD Connector 目录禁用远程身份验证拨入用户服务 (RADIUS) 服务器的多重验证 (MFA) 的权限	写入	directory*		
DisableRoleAccess[仅权限]	授予禁用 Amazon 目录中身份 Amazon Web Services Management Console 访问权限的权限	写入	directory*		
DisableSso	授予禁用目录的 Single Sign-On 的权限	写入	directory*		
EnableClientAuthentication	授予启用指定目录的替代客户端身份验证方法的权限	写入	directory*		
EnableDirectoryDataAccess	授予权限以启用指定目录的 Directory Service Data API	写入	directory*		
EnableLDAPS	授予激活特定目录的开关以始终使用 LDAP 安全调用的权限	写入	directory*		
EnableRadius	授予针对 AD Connector 目录启用远程身份验证拨入用户服务 (RADIUS) 服务器的多重验证 (MFA) 的权限	写入	directory*		
EnableRoleAccess[仅权限]	授予权限以允许 Amazon Web Services Management Console 访问您的 “ Amazon 目录” 中的身份	写入	directory*		iam:PassRole

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
EnableSso	授予启用目录的 Single Sign-On 的权限	写入	directory*		
GetAuthorizedApplicationDetails[仅权限]	授予检索目录上的授权应用程序详细信息的权限	读取	directory*		
GetDirectoryLimits	授予获取当前区域的目录限制信息的权限	读取			
GetSnapshotLimits	授予获取目录的手动快照限制的权限	读取	directory*		
ListAuthorizedApplications[仅权限]	授予获取目录授权的 Amazon 应用程序的权限	读取	directory*		
ListCertificates	授予列出在指定目录的安全 LDAP 连接中注册的所有证书的权限	列表	directory*		
ListIpRoutes	授予列出您为目录添加的地址块的权限	读取	directory*		
ListLogSubscriptions	授予列出活动日志订阅的权限 Amazon Web Services 账户	读取			
ListSchemaExtensions	授予列出应用于 Microsoft AD 目录的所有架构扩展的权限	列表	directory*		
ListTagsForResource	授予列出 Amazon Directory Services 目录上的所有标签的权限	读取	directory*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
RegisterCertificate	授予在安全的 LDAP 连接中注册证书的权限	写入	directory*		
RegisterEventTopic	授予将目录与 SNS 主题关联的权限	写入	directory*		sns:GetTopicAttributes
RejectSharedDirectory	授予拒绝从目录所有者账户中发送的目录共享请求的权限	写入	directory*		
RemoveIpRoutes	授予从目录中删除 IP 地址块的权限	写入	directory*		
RemoveRegion	授予停止所有复制并从指定区域中删除域控制器的权限。使用此操作无法删除主区域	写入	directory*		
RemoveTagsFromResource	授予从 Amazon Directory Services 目录中删除标签的权限	标记	directory*		ec2:DeleteTags
				aws:RequestTag/${TagKey} aws:TagKeys	
ResetUserPassword	授予重置你 Amazon 托管的 Microsoft AD 或 Simple AD 目录中任何用户的密码的权限	写入	directory*		
RestoreFromSnapshot	授予使用现有目录快照恢复目录的权限	写入	directory*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ShareDirectory	授予与另一个 Amazon Web Services 账户（目录使用者）共享您 Amazon Web Services 账户（目录所有者）中指定目录的权限。通过此操作，您可以从任何一个 Amazon VPC 中使用您的目录，也可以从任何 Amazon Web Services 账户 一个 Amazon VPC 中使用您的目录 Amazon Web Services 区域	写入	directory*		
StartSchemaExtension	授予将架构扩展应用于 Microsoft AD 目录的权限	写入	directory*		
UnauthorizeApplication[仅权限]	授予从您的 Amazon 目录中取消对应用程序的授权的权限	写入	directory*		
UnshareDirectory	授予停止目录所有者与使用者账户之间的目录共享的权限	写入	directory*		
UpdateAuthorizedApplication[仅权限]	授予更新您的 Amazon 目录的授权应用程序的权限	写入	directory*		
UpdateConditionalForwarder	授予更新已为您的 Amazon 目录设置的条件转发器的权限	写入	directory*		
UpdateDirectory[仅权限]	授予权限以更新指定目录的配置（例如服务账户凭证或 DNS 服务器 IP 地址）	写入	directory*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateDirectorySetup	授予权限以更新特定更新类型的目录	写入	directory*		
UpdateNumberOfDomainControllers	授予在目录中添加或删除域控制器的权限 根据当前值和新值（通过该 API 调用提供）之间的差异，将添加或删除域控制器。在更新了请求数量的域控制器后，最多可能需要 45 分钟才能完全激活任何新的域控制器。在此期间，您无法发出其他更新请求	写入	directory*		
UpdateRadius	授予更新 AD Connector 目录的远程身份验证拨入用户服务 (RADIUS) 服务器信息的权限	写入	directory*		
UpdateSettings	授予更新指定目录的可配置设置的权限	写入	directory*		
UpdateTrust	授予更新已在你的 Amazon 托管 Microsoft AD 目录和本地活动目录之间建立的信任的权限	写入	directory*		
VerifyTrust	授予权限以验证你在 Amazon 云端的 Microsoft AD 与外部域之间的信任关系	读取	directory*		

Amazon Directory Service 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
directory	arn:${Partition}:ds:${Region}:${Account}:directory/${DirectoryId}	aws:ResourceTag/${TagKey}

Amazon Directory Service 的条件键

Amazon Directory Service 定义了以下可以在 IAM 策略Condition元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按对 Amazon DS 的请求值筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按正在处理的 Amazon DS 资源筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString

Amazon DynamoDB 的操作、资源和条件键

Amazon DynamoDB（服务前缀：dynamodb）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon DynamoDB 定义的操作

- Amazon DynamoDB 定义的资源类型
- Amazon DynamoDB 的条件键

Amazon DynamoDB 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchGetItem	授予权限以从一个或多个表中返回一个或多个项目的属性	读取	table*		
				dynamodb:Attributes	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:Select	
BatchWriteItem	授予权限以将多个项目放入一个或多个表中或将其删除	写入	table*		
				dynamodb:Attributes dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity	
ConditionCheckItem	授予 ConditionCheckItem 操作权限，检查具有给定主键的项目是否存在一组属性	读取	table*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				dynamodb:Attributes dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
CreateBackup	授予权限以创建现有表的备份	写入	table*		
CreateGlobalTable	授予权限以从现有表创建全局表	写入	global-table*		
			table*		
CreateTable	授予 CreateTable 操作权限，为您的账户添加新表	写入	table*		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateTableReplica[仅权限]	授予权限以添加新的副本表	写入	table*		
DeleteBackup	授予权限以删除现有表的备份	写入	backup*		
DeleteItem	授予按主键删除表中单个项目的权限	写入	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
DeleteResourcePolicy	授予权限以删除附加到资源中的资源策略	权限管理	stream*		
			table*		
DeleteTable	向删除表及其所有项目的 DeleteTable 操作授予权限	写入	table*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteTableReplica[仅权限]	授予权限以删除副本表及其所有项目	写入	table*		
DescribeBackup	授予权限以描述现有表的备份	读取	backup*		
DescribeContinuousBackups	授予权限以检查指定表上的备份还原设置的状态	读取	table*		
DescribeContributorInsights	授予权限以描述给定表或全局二级索引的 Contributor Insights 状态和相关详细信息	读取	table*		
			index		
DescribeEndpoints	授予返回区域端点信息的权限	读取			
DescribeExport	授予权限以描述现有表的导出	读取	export*		
DescribeGlobalTable	授予返回指定全局表相关信息的权限	读取	global-table*		
DescribeGlobalTableSettings	授予返回指定全局表相关设置信息的权限	读取	global-table*		
DescribeImport	授予描述某个现有导入的权限	读取	import*		
DescribeKinesisStreamingDestination	授予权限以授予描述给定表的 Kinesis 流式传输状态和相关详细信息的权限	读取	table*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeLimits	授予返回您在某个区域的当前预配置容量限制的权限，包括整个区域以及您在 Amazon Web Services 账户 该区域创建的任何 DynamoDB 表的当前预配置容量限制	读取			
DescribeReservedCapacity[仅权限]	授予权限以描述一个或多个购买的预留容量	读取			
DescribeReservedCapacityOfferings[仅权限]	授予权限以描述可供购买的预留容量产品	读取			
DescribeStream	授予权限以返回有关流的信息，包括流的当前状态、其 Amazon Resource Name (ARN)、其分片的构成及其相应的 DynamoDB 表	读取	stream*		
DescribeTable	授予权限以返回有关表的信息	读取	table*		
DescribeTableReplicaAutoScaling	授予权限以描述全局表的所有副本之间的弹性伸缩设置	读取	table*		
DescribeTimeToLive	授予权限以给出指定表的存活时间 (TTL) 状态的描述	读取	table*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DisableKinesisStreamingDestination	授予权限以授予停止从 DynamoDB 表到 Kinesis 数据流的复制的权限	写入	table*		
EnableKinesisStreamingDestination	授予权限以授予在启用工作流期间选择的时间戳启动将表数据复制到指定 Kinesis 数据流的权限	写入	table*		
ExportTableToPointInTime	授予权限以启动将 DynamoDB 表到 S3 的导出过程	写入	table*		
GetAbacStatus[仅权限]	授予查看账户基于属性的访问控制状态的权限	读取			
GetItem	授予 GetItem 操作权限，该操作返回具有给定主键的项目的一组属性	读取	table*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:Select	
GetRecords	授予权限以检索给定分片中的流记录	读取	stream*		
GetResourcePolicy	授予权限以查看资源的资源策略	读取	stream* table*		
GetShardIterator	授予返回分片迭代器的权限	读取	stream*		
ImportTable	授予将某个导入从 S3 启动到某个 DynamoDB 表的权限	写入	table*		
ListBackups	授予权限以列出与账户和终端节点关联的备份	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListContributorInsights	授予列出与当前账户和终端节点关联的所有表和全局二级索引的权限 ContributorInsightsSummary	列表			
ListExports	授予权限以列出与账户和终端节点关联的导出	列表			
ListGlobalTables	授予权限以列出在指定区域中具有副本的所有全局表	列表			
ListImports	授予列出与账户和端点关联的导入的权限	列表			
ListStreams	授予返回与当前账户和端点 ARNs 关联的直播数组的权限	读取			
ListTables	授予权限以返回与当前账户和终端节点关联的表名称的数组	列表			
ListTagsOfResource	授予权限以列出 Amazon DynamoDB 资源上的所有标签	读取	table*		
PartiQLDelete	授予按主键删除表中单个项目的权限	Write	table*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnValues	
PartiQLInsert	授予在表中不存在具有相同主键的项目时创建新项目的权限	Write	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys	
PartiQLSelect	授予读取表或索引中项目的一组属性的权限	Read	table*		
			index		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:FullTableScan dynamodb:LeadingKeys dynamodb:Select	
PartiQLUpdate	授予编辑现有项目属性的权限	写入	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnValues	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PurchaseReservedCapacityOfferings[仅权限]	授予权限以购买预留容量用于您的账户	写入			
PutItem	授予权限以创建新项目，或将旧项目替换为新项目	写入	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
PutResourcePolicy	授予权限以将资源策略附加到资源	权限管理	stream*		
			table*		
Query	授予权限以使用表的主键或二级索引直接访问该表或索引中的项目	读取	table*		
			index		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				dynamodb:Attributes dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues dynamodb:Select	
RestoreTableFromAwsBackup[仅权限]	授予从 B Amazon ackup 上的恢复点创建新表的权限	写入	table*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
RestoreTableFromBackup	授予权限以从现有备份中创建新表	写入	backup*		dynamodb:BatchWriteItem dynamodb:DeleteItem dynamodb:GetItem dynamodb:PutItem dynamodb:Query dynamodb:Scan dynamodb:UpdateItem
			table*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
RestoreTableToPointInTime	授予权限以将表还原到某个时间点	写入	table*		dynamodb:BatchWriteItem dynamodb:DeleteItem dynamodb:GetItem dynamodb:PutItem dynamodb:Query dynamodb:Scan dynamodb:UpdateItem
Scan	授予权限以通过访问表或者二级索引中的每个项目，返回一个或多个项目和项目属性	读取	table*		
			index		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				dynamodb:Attributes dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues dynamodb:Select	
StartAwsBackupJob[仅权限]	授予在启用高级功能的情况下在 Bac Amazon kup 上创建备份的权限	写入	table*		
TagResource	授予权限以将一组标签与 Amazon DynamoDB 资源关联	标记	table*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予权限从 Amazon DynamoDB 资源中删除标签的关联	标记	table*		
				aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateAbacStatus[仅权限]	授予更新账户基于属性的访问控制状态的权限	权限管理			
UpdateContinuousBackups	授予权限以启用或禁用连续备份	写入	table*		
UpdateContributorInsights	授予权限以更新特定表或全局二级索引的 Contributor Insights 状态	写入	table*		
			index		
UpdateGlobalTable	授予权限以在指定的全局表中添加或删除副本	写入	global-table*		
			table*		
UpdateGlobalTableSettings	授予更新指定全局表的设置的权限	写入	global-table*		
			table*		
UpdateGlobalTableVersion[仅权限]	授予更新指定全局表的版本的权限	写入	global-table*		
			table		
UpdateItem	授予权限以编辑现有项目的属性，或者将新项目添加到表中（如果它不存在）	写入	table*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
UpdateKinesisStreamingDestination	授予权限以更新指定 Kinesis 数据流的数据复制配置	写入	table*		
UpdateTable	授予权限以修改给定表的预置吞吐量设置、全局二级索引或 DynamoDB Streams 设置	写入	table*		
UpdateTableReplicaAutoScaling	授予权限以更新副本表上的自动伸缩设置	写入	table*		
UpdateTimeToLive	授予权限以为指定表启用或禁用 TTL	写入	table*		

Amazon DynamoDB 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
index	arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/index/${IndexName}	aws:ResourceTag/${TagKey}
stream	arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/stream/${StreamLabel}	
table	arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}	aws:ResourceTag/${TagKey}
backup	arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/backup/${BackupName}	
export	arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/export/${ExportName}	
global-table	arn:${Partition}:dynamodb::${Account}:global-table/${GlobalTableName}	
import	arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/import/${ImportName}	

Amazon DynamoDB 的条件键

Amazon DynamoDB 定义了以下可以在 IAM policy 的 `Condition` 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

> **Note**
>
> 有关如何使用上下文键通过 IAM policy 优化 DynamoDB 访问的信息，请参阅《Amazon DynamoDB 开发人员指南》中的使用 IAM policy 条件实现精细访问控制。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString
dynamodb:Attributes	通过表的属性（字段或列）名称筛选访问权限	ArrayOfString
dynamodb:EnclosingOperation	通过屏蔽事务 APIs 调用来过滤访问权限并允许非交易 APIs 调用，反之亦然	字符串
dynamodb:FullTableScan	通过阻止全表扫描筛选访问权限	布尔型
dynamodb:LeadingKeys	根据表的分区键筛选访问权限	ArrayOfString

条件键	描述	类型
dynamodb:ReturnConsumedCapacity	按请求的 ReturnConsumedCapacity 参数筛选访问权限。包含“TOTAL”或“NONE”	字符串
dynamodb:ReturnValues	按请求 ReturnValues 参数筛选访问权限。包含下列项之一：“ALL_OLD”、“UPDATED_OLD”、“ALL_NEW”、“UPDATED_NEW”或“NONE”	字符串
dynamodb:Select	根据 Query 或 Scan 请求的 Select 参数筛选访问权限	字符串

Amazon DynamoDB Accelerator (DAX) 的操作、资源和条件键

Amazon DynamoDB Accelerator (DAX)（服务前缀：dax）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon DynamoDB Accelerator (DAX) 定义的操作
- Amazon DynamoDB Accelerator (DAX) 定义的资源类型
- Amazon DynamoDB Accelerator (DAX) 的条件键

Amazon DynamoDB Accelerator (DAX) 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchGetItem	授予权限以从一个或多个表中返回一个或多个项目的属性	读取	application*		
BatchWriteItem	授予权限以将多个项目放入一个或多个表中或将其删除	写入	application*		
ConditionCheckItem	向使用给定主键检查项目是否存在一组属性的 ConditionCheckItem 操作授予权限	读取	application*		
CreateCluster	授予权限以创建 DAX 集群	写入	application*		dax:CreateParameterGroup

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
					dax:CreateSubnetGroup ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:GetRole iam:PassRole

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateParameterGroup	授予权限以创建参数组	写入			
CreateSubnetGroup	授予权限以创建子网组	写入			
DecreaseReplicationFactor	授予权限以从 DAX 集群删除一个或多个节点	写入	application*		
DeleteCluster	授予权限以删除以前预配置的 DAX 集群	写入	application*		
DeleteItem	授予按主键删除表中单个项目的权限	写入	application*		
				dax:EnclosingOperation	
DeleteParameterGroup	授予权限以删除指定的参数组	写入			
DeleteSubnetGroup	授予权限以删除子网组	写入			
DescribeClusters	授予权限以返回有关所有预置 DAX 集群的信息	列表	application		
DescribeDefaultParameters	授予权限以返回 DAX 的默认系统参数信息	列表			
DescribeEvents	授予权限以返回与 DAX 集群和参数组相关的事件	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeParameterGroups	授予权限以返回参数组描述列表	列表			
DescribeParameters	授予权限以返回特定参数组的详细参数列表	读取			
DescribeSubnetGroups	授予权限以返回子网组描述列表	列表			
GetItem	授予 GetItem 操作权限，该操作返回具有给定主键的项目的一组属性	读取	application*		
				dax:EnclosingOperation	
IncreaseReplicationFactor	授予权限以将一个或多个节点添加到 DAX 集群	写入	application*		
ListTags	授予权限以返回 DAX 集群所有标签的列表	读取	application*		
PutItem	授予权限以创建新项目，或将旧项目替换为新项目	写入	application*		
				dax:EnclosingOperation	
Query	授予权限以使用表的主键或二级索引直接访问该表或索引中的项目	读取	application*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
RebootNode	授予权限以重启 DAX 集群的单个节点	写入	application*		
Scan	授予权限以通过访问表或者二级索引中的每个项目，返回一个或多个项目和项目属性	读取	application*		
TagResource	授予权限以将一组标签与 DAX 资源关联	标记	application*		
UntagResource	授予权限以从 DAX 资源中删除标签的关联	标记	application*		
UpdateCluster	授予权限以修改 DAX 集群的设置	写入	application*		
UpdateItem	授予权限以编辑现有项目的属性，或者将新项目添加到表中（如果它不存在）	写入	application*		
				dax:EnclosingOperation	
UpdateParameterGroup	授予权限以修改参数组的参数	写入			
UpdateSubnetGroup	授予权限以修改现有子网组	写入			

Amazon DynamoDB Accelerator (DAX) 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从

而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
application	`arn:${Partition}:dax:${Region}:${Account}:cache/${ClusterName}`	

Amazon DynamoDB Accelerator (DAX) 的条件键

Amazon DynamoDB Accelerator (DAX) 定义以下可以在 IAM policy 的 `Condition` 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
dax:EnclosingOperation	用于阻止交易 APIs 呼叫并允许非交易 APIs 调用，反之亦然	字符串

Amazon A EC2 uto Scaling 的操作、资源和条件密钥

Amazon A EC2 uto Scaling（服务前缀:`autoscaling`）提供以下特定于服务的资源、操作和条件上下文密钥以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- 由 Amazon A EC2 uto Scaling 定义的操作
- 由 Amazon A EC2 uto Scaling 定义的资源类型
- Amazon A EC2 uto Scaling 的条件密钥

由 Amazon A EC2 uto Scaling 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AttachInstances	授予将一个或多个 EC2 实例附加到指定的 Auto Scaling 组的权限	写入	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AttachLoadBalancerTargetGroups	授予将一个或多个目标组附加到指定的 Auto Scaling 组的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TargetGroupARNs	
AttachLoadBalancers	授予将一个或多个负载均衡器附加到指定的 Auto Scaling 组的权限	写入	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:LoadBalancerNames	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AttachTrafficSources	授予将一个或多个流量源附加到附加自动扩缩组的权限	写入	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TrafficSourceIdentifiers	
BatchDeleteScheduledAction	授予删除指定的计划操作的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
BatchPutScheduledUpdateGroupAction	授予为 Auto Scaling 组创建或更新多个计划扩展操作的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CancelInstanceRefresh	授予权限以取消正在进行的实例刷新操作	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
CompleteLifecycleAction	授予使用指定结果完成指定令牌或实例的生命周期操作的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
CreateAutoScalingGroup	授予使用指定名称和属性创建 Auto Scaling 组的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	iam:CreateServiceLinkedRole iam:PassRole

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				autoscaling:CapacityReservationIds autoscaling:CapacityReservationResourceGroupArns autoscaling:InstanceTypes autoscaling:LaunchConfigurationName autoscaling:LaunchTemplateVersionSpecified autoscaling:LoadBalancerNames	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				autoscaling:MaxSize autoscaling:MinSize autoscaling:TargetGroupARNs autoscaling:TrafficSourceIdentifiers autoscaling:VPCZoneIdentifiers aws:RequestTag/${TagKey} aws:TagKeys	
CreateLaunchConfiguration	授予创建启动配置的权限	Write	launchConfiguration*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				autoscaling:ImageId autoscaling:InstanceType autoscaling:SpotPrice autoscaling:MetadataHttpTokens autoscaling:MetadataHttpPutResponseHopLimit autoscaling:MetadataHttpEndpoint	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateOrUpdateTags	授予创建或更新与指定 Auto Scaling 组关联的标签的权限	Tagging	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAutoScalingGroup	授予删除指定 Auto Scaling 组的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteLaunchConfiguration	授予删除指定启动配置的权限	Write	launchConfiguration*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteLifecycleHook	授予删除指定生命周期挂钩的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteNotificationConfiguration	授予删除指定通知的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeletePolicy	授予删除指定 Auto Scaling 策略的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteScheduledAction	授予删除指定计划操作的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteTags	授予删除指定标签的权限	Tagging	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteWarmPool	授予删除与 Auto Scaling 组关联的热资源池的权限	写入	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DescribeAccountLimits	授予描述您的当前 Auto Scaling 资源限制的权限 Amazon Web Services 账户	列表			
DescribeAdjustmentTypes	授予描述政策调整类型的权限，以便与一起使用 PutScalingPolicy	列表			
DescribeAutoScalingGroups	授予描述一个或多个 Auto Scaling 组的权限。如果未提供名称列表，则调用将描述所有 Auto Scaling 组	List			
DescribeAutoScalingInstances	授予描述一个或多个 Auto Scaling 实例的权限。如果未提供列表，则调用将描述所有实例	List			
DescribeAutoScalingNotificationTypes	授予描述 Auto Scaling 支持的通知类型的权限	List			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeInstanceRefreshes	授予权限以描述 Auto Scaling 组的一个或多个实例刷新	List			
DescribeLaunchConfigurations	授予描述一个或多个启动配置的权限。如果您省略了名称列表，则调用将描述所有启动配置	List			
DescribeLifecycleHookTypes	授予描述可用的生命周期挂钩类型的权限	List			
DescribeLifecycleHooks	授予描述指定 Auto Scaling 组的生命周期挂钩的权限	List			
DescribeLoadBalancerTargetGroups	授予描述指定 Auto Scaling 组的目标组的权限	List			
DescribeLoadBalancers	授予描述指定 Auto Scaling 组的负载均衡器的权限	列表			
DescribeMetricCollectionTypes	授予描述 Auto Scaling 可用 CloudWatch 指标的权限	列表			
DescribeNotificationConfigurations	授予描述与指定 Auto Scaling 组关联的通知操作的权限	List			
DescribePolicies	授予描述指定 Auto Scaling 组的策略的权限	List			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeScalingActivities	授予描述指定 Auto Scaling 组的一个或多个扩缩活动的权限	列表			
DescribeScalingProcessTypes	授予描述用于 ResumeProcesses 和的扩展过程类型的权限 SuspendProcesses	列表			
DescribeScheduledActions	授予描述已为您的 Auto Scaling 组计划但尚未运行的操作的权限	List			
DescribeTags	授予描述指定标签的权限	Read			
DescribeTerminationPolicyTypes	授予描述 Auto Scaling 支持的终止策略的权限	列表			
DescribeTrafficSources	授予描述指定 Auto Scaling 组的目标组的权限	列表			
DescribeWarmPool	授予描述与 Auto Scaling 组关联的热资源池的权限	List			
DetachInstances	授予从指定 Auto Scaling 组删除一个或多个实例的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DetachLoadBalancerTargetGroups	授予从指定 Auto Scaling 组分离一个或多个目标组的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TargetGroupARNs	
DetachLoadBalancers	授予从指定 Auto Scaling 组删除一个或多个负载均衡器的权限	写入	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:LoadBalancerNames	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DetachTrafficSources	授予将一个或多个流量源从自动扩缩组分离的权限	写入	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TrafficSourceIdentifiers	
DisableMetricsCollection	授予禁用对指定 Auto Scaling 组的指定指标的监控的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
EnableMetricsCollection	授予启用对指定 Auto Scaling 组的指定指标的监控的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
EnterStandby	授予将指定实例移动到备用模式的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
ExecutePolicy	授予执行指定策略的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
ExitStandby	授予将指定实例移出备用模式的权限	写入	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
GetPredictiveScalingForecast	授予权限以检索预测性扩展策略的预测数据	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutLifecycleHook	授予权限以为指定 Auto Scaling 组创建或更新生命周期钩子	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
PutNotificationConfiguration	授予配置 Auto Scaling 组以在发生指定事件时发送通知的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
PutScalingPolicy	授予为 Auto Scaling 组创建或更新策略的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutScheduledUpdateGroupAction	授予为 Auto Scaling 组创建或更新计划的扩展操作的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:MaxSize autoscaling:MinSize	
PutWarmPool	授予创建或更新与指定 Auto Scaling 组关联的暖资源池的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
RecordLifecycleActionHeartbeat	授予记录与指定令牌或实例关联的生命周期操作的检测信号的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
ResumeProcesses	授予恢复指定 Auto Scaling 组的指定已暂停 Auto Scaling 流程或所有已暂停流程的权限	写入	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
RollbackInstanceRefresh	授予回滚正在进行的实例刷新操作的权限	写入	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
SetDesiredCapacity	授予设置指定 Auto Scaling 组的大小的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
SetInstanceHealth	授予查看指定实例的运行状态的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
SetInstanceProtection	授予更新指定实例的实例保护设置的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StartInstanceRefresh	授予权限以启动新实例刷新操作	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
SuspendProcesses	授予暂停指定 Auto Scaling 组的指定 Auto Scaling 流程或所有流程的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
TerminateInstanceInAutoScalingGroup	授予终止指定实例及选择性地调整所需组大小的权限	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateAutoScalingGroup	授予更新指定 Auto Scaling 组的配置的权限	写入	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	iam:PassRole

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				autoscaling:CapacityReservationIds autoscaling:CapacityReservationResourceGroupArns autoscaling:InstanceTypes autoscaling:LaunchConfigurationName autoscaling:LaunchTemplateVersionSpecified autoscaling:MaxSize autoscaling:MinSize	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				autoscaling:VPCZoneIdentifiers	

由 Amazon A EC2 uto Scaling 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}	

Amazon A EC2 uto Scaling 的条件密钥

Amazon A EC2 uto Scaling 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素中。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
autoscaling:CapacityReservationIds	根据容量预留筛选访问权限 IDs	ArrayOfString
autoscaling:CapacityReservationResourceGroupArns	根据容量预留资源组的 ARN 筛选访问权限	ArrayOfString
autoscaling:ImageId	根据启动配置的 AMI ID 筛选访问权限	字符串
autoscaling:InstanceType	根据启动配置的实例类型筛选访问权限	字符串
autoscaling:InstanceTypes	根据作为混合实例策略启动模板替代的实例类型筛选访问权限。使用其来限定可以在策略中明确定义哪些实例类型	字符串
autoscaling:LaunchConfigurationName	根据启动配置的名称筛选访问权限	字符串
autoscaling:LaunchTemplateVersionSpecified	根据用户是可以指定启动模板的任何版本，还是只能指定“最新”或“原定设置”版本来筛选访问权限	Bool
autoscaling:LoadBalancerNames	根据负载均衡器的名称筛选访问权限	ArrayOfString
autoscaling:MaxSize	根据请求中的最大扩缩大小筛选访问权限	数值

条件键	描述	类型
autoscaling:MetadataHttpEndpoint	根据是否为实例元数据服务启用 HTTP 终端节点来筛选访问权限	字符串
autoscaling:MetadataHttpPutResponseHopLimit	根据调用实例元数据服务时允许的跃点数筛选访问权限	数值
autoscaling:MetadataHttpTokens	根据调用实例元数据服务时是否需要令牌（可选或必需）筛选访问权限	字符串
autoscaling:MinSize	根据请求中的最小扩缩大小筛选访问权限	数值
autoscaling:ResourceTag/${TagKey}	根据与资源关联的标签筛选访问	字符串
autoscaling:SpotPrice	根据启动配置的 Spot 实例的价格筛选访问权限	数值
autoscaling:TargetGroupARNs	根据目标组的 ARN 筛选访问权限	ArrayOfARN
autoscaling:TrafficSourceIdentifiers	根据流量源的标识符筛选访问权限	ArrayOfString
autoscaling:VPCZoneIdentifiers	根据 VPC 区域的标识符筛选访问权限	ArrayOfString

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中传递的标签筛选访问	字符串
aws:ResourceTag/${TagKey}	根据与资源关联的标签筛选访问	字符串
aws:TagKeys	根据在请求中传递的标签键筛选访问	ArrayOfString

Amazon EC2 Image Builder 的操作、资源和条件密钥

Amazon EC2 Image Builder（服务前缀:`imagebuilder`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- 由亚马逊 EC2 Image Builder 定义的操作
- 由 Amazon EC2 Image Builder 定义的资源类型
- Amazon EC2 Image Builder 的条件密钥

由亚马逊 EC2 Image Builder 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须

具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CancelImageCreation	授予权限以取消映像创建	写入	image*		
CancelLifecycleExecution	授予取消生命周期执行的权限	写入	lifecycleExecution*		
CreateComponent	授予权限以创建新组件	Write	component*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole imagebuilder:TagResource kms:Encrypt

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
					kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateContainerRecipe	授予权限以创建新的容器配方	Write	containerRecipe*	aws:RequestTag/${TagKey} aws:TagKeys	ecr:DescribeImages ecr:DescribeRepositories iam:CreateServiceLinkedRole imagebuilder:GetComponent imagebuilder:GetImage imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateDistributionConfiguration	授予权限以创建新的分配配置	Write	distributionConfiguration*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole imagebuilder:TagResource

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateImage	授予权限以创建新的映像	Write	image*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe imagebuilder:GetInfrastructureConfiguration imagebuilder:GetWorkflow

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
					imagebuilder:TagResource

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateImagePipeline	授予权限以创建新的映像管道	Write	imagePipeline*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe imagebuilder:GetInfrastructureConfiguration imagebuilder:GetWorkflow

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
					imagebuilder:TagResource
CreateImageRecipe	授予权限以创建新的映像配方	Write	imageRecipe*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeImages iam:CreateServiceLinkedRole imagebuilder:GetComponent imagebuilder:GetImage imagebuilder:TagResource

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateInfrastructureConfiguration	授予权限以创建新的基础设施配置	写入	infrastructureConfiguration*	aws:RequestTag/${TagKey} aws:TagKeys imagebuilder:CreatedResourceTagKeys imagebuilder:CreatedResourceTag/<key> imagebuilder:Ec2MetadataHttpTokens imagebuilder:StatusTopicArn	iam:CreateServiceLinkedRole iam:PassRole imagebuilder:TagResource sns:Publish

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateLifecyclePolicy	授予创建新生命周期策略的权限	写入	lifecyclePolicy*	aws:RequestTag/${TagKey} aws:TagKeys imagebuilder:LifecyclePolicyResourceType	iam:PassRole imagebuilder:TagResource
CreateWorkflow	授予创建新工作流的权限	写入	workflow*	aws:RequestTag/${TagKey} aws:TagKeys	imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext s3:GetObject s3:ListBucket

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteComponent	授予删除组件的权限	Write	component*		
DeleteContainerRecipe	授予删除容器配方的权限	Write	containerRecipe*		
DeleteDistributionConfiguration	授予权限以删除分配配置	Write	distributionConfiguration*		
DeleteImage	授予权限以删除映像	Write	image*		
DeleteImagePipeline	授予权限以删除映像管道	Write	imagePipeline*		
DeleteImageRecipe	授予权限以删除映像配方	Write	imageRecipe*		
DeleteInfrastructureConfiguration	授予权限以删除基础设施配置	写入	infrastructureConfiguration*		
DeleteLifecyclePolicy	授予删除生命周期策略的权限	写入	lifecyclePolicy*		
DeleteWorkflow	授予权限以删除工作流程	写入	workflow*		
GetComponent	授予权限以查看有关组件的详细信息	Read	component*		kms:Decrypt
GetComponentPolicy	授予权限以查看与组件关联的资源策略	Read	component*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetContainerRecipe	授予权限以查看有关容器配方的详细信息	Read	containerRecipe*		
GetContainerRecipePolicy	授予权限以查看与容器配方关联的资源策略	Read	containerRecipe*		
GetDistributionConfiguration	授予权限以查看有关分配配置的详细信息	Read	distributionConfiguration*		
GetImage	授予权限以查看有关映像的详细信息	Read	image*	aws:ResourceTag/${TagKey}	
GetImagePipeline	授予权限以查看有关映像管道的详细信息	Read	imagePipeline*		
GetImagePolicy	授予权限以查看与映像关联的资源策略	Read	image*		
GetImageRecipe	授予权限以查看有关映像配方的详细信息	Read	imageRecipe*		
GetImageRecipePolicy	授予权限以查看与映像配方关联的资源策略	Read	imageRecipe*		
GetInfrastructureConfiguration	授予权限以查看有关基础设施配置的详细信息	读取	infrastructureConfiguration*		
GetLifecycleExecution	授予查看生命周期执行详细信息的权限	读取	lifecycleExecution* -		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetLifecyclePolicy	授予查看生命周期策略详细信息的权限	读取	lifecyclePolicy*		
GetMarketplaceResource	授予检索 Marketplace 提供的资源的权限	读取	component*		
GetWorkflow	授予查看工作流详细信息的权限	读取	workflow*		kms:Decrypt
GetWorkflowExecution	授予查看工作流程执行详细信息的权限	读取	workflowExecution*		
GetWorkflowStepExecution	授予查看工作流程步骤执行详细信息的权限	读取	workflowStepExecution*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ImportComponent	授予权限以导入新组件	写入	component *	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ImportDiskImage	授予导入磁盘映像的权限	写入	imageVersion*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetInfrastructureConfiguration imagebuilder:GetWorkflow imagebuilder:TagResource s3:GetObject s3:ListBucket

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ImportVmImage	授予导入镜像的权限	写入	imageVersion*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeImages ec2:DescribeImportImageTasks iam:CreateServiceLinkedRole
ListComponentBuildVersions	授予权限以列出您账户中的组件内部版本	List	componentVersion*		
ListComponents	授予权限以列出您的账户拥有或与之共享的组件版本	List			
ListContainerRecipes	授予权限以列出您账户拥有或与之共享的容器配方	List			
ListDistributionConfigurations	授予权限以列出您账户中的分配配置	List			
ListImageBuildVersions	授予权限以列出您账户中的映像内部版本	列表	imageVersion*		
ListImagePackages	授予权限以返回指定映像上安装的软件包列表	列表	image*	aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListImagePipelineImages	授予权限以返回由指定管道创建的映像的列表	列表	imagePipeline*		
ListImagePipelines	授予权限以列出您账户中的映像管道	List			
ListImageRecipes	授予权限以列出您账户拥有或与之共享的映像配方	列表			
ListImageScanFindingAggregations	授予权限以列出您账户中的映像扫描结果的聚合	列表	image		
			imagePipeline		
ListImageScanFindings	授予权限以列出您账户中的映像的扫描结果	列表	image		inspector2:ListFindings
			imagePipeline		
ListImages	授予权限以列出您账户拥有或与之共享的映像版本	List			
ListInfrastructureConfigurations	授予权限以列出您账户中的基础设施配置	列表			
ListLifecycleExecutionResources	授予列出指定生命周期执行的资源的权限	列表	lifecycleExecution*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListLifecycleExecutions	授予列出指定资源的生命周期执行的权限	列表	image		
			lifecyclePolicy		
ListLifecyclePolicies	授予列出您账户中的生命周期策略的权限	列表			
ListTagsForResource	授予权限以列出 Image Builder 资源的标签	读取	component	aws:ResourceTag/${TagKey}	
			containerRecipe	aws:ResourceTag/${TagKey}	
			distributionConfiguration	aws:ResourceTag/${TagKey}	
			image	aws:ResourceTag/${TagKey}	
			imagePipeline	aws:ResourceTag/${TagKey}	
			imageRecipe	aws:ResourceTag/${TagKey}	
			infrastructureConfiguration	aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			lifecyclePolicy	aws:ResourceTag/${TagKey}	
			workflow	aws:ResourceTag/${TagKey}	
ListWaitingWorkflowSteps	授予列出调用方账户的等待工作流步骤的权限	列表			
ListWorkflowBuildVersions	授予列出您账户中的工作流内部版本的权限	列表	workflowVersion*		
ListWorkflowExecutions	授予权限以列出指定映像的工作流程执行情况	列表	image*		
ListWorkflowStepExecutions	授予权限以列出指定工作流程的步骤执行情况	列表	workflowExecution*		
ListWorkflows	授予列出您账户拥有或与之共享的工作流版本的权限	列表			
PutComponentPolicy	授予权限以设置与组件关联的资源策略	Permissions management	component*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutContainerRecipePolicy	授予权限以设置与容器配方关联的资源策略	Permissions management	containerRecipe*		
PutImagePolicy	授予权限以设置与映像关联的资源策略	Permissions management	image*		
PutImageRecipePolicy	授予权限以设置与映像配方关联的资源策略	权限管理	imageRecipe*		
SendWorkflowStepAction	授予将操作发送到工作流步骤的权限	写入	image* workflowStepExecution*		
StartImagePipelineExecution	授予权限以从管道创建新的映像	写入	imagePipeline*		iam:CreateServiceLinkedRole imagebuilder:GetImagePipeline
StartResourceStateUpdate	授予启动指定资源的状态更新的权限	写入	image*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
TagResource	授予权限以标记 Image Builder 资源	Tagging	component	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			containerRecipe	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			distributionConfiguration	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			image	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			imagePipeline	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			imageRecipe	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			infrastructureConfiguration	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			lifecyclePolicy	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			workflow	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UntagResource	授予权限以取消标记 Image Builder 资源	Tagging	component	aws:ResourceTag/${TagKey} aws:TagKeys	
			containerRecipe	aws:ResourceTag/${TagKey} aws:TagKeys	
			distributionConfiguration	aws:ResourceTag/${TagKey} aws:TagKeys	
			image	aws:ResourceTag/${TagKey} aws:TagKeys	
			imagePipeline	aws:ResourceTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			imageRecipe	aws:ResourceTag/${TagKey} aws:TagKeys	
			infrastructureConfiguration	aws:ResourceTag/${TagKey} aws:TagKeys	
			lifecyclePolicy	aws:ResourceTag/${TagKey} aws:TagKeys	
			workflow	aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateDistributionConfiguration	授予权限以更新现有分配配置	Write	distributionConfiguration*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateImagePipeline	授予权限以更新现有映像管道	Write	imagePipeline*		iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe imagebuilder:GetInfrastructureConfiguration imagebuilder:GetWorkflow

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateInfrastructureConfiguration	授予权限以更新现有基础设施配置	写入	infrastructureConfiguration*	aws:ResourceTag/${TagKey} imagebuilder:CreatedResourceTagKeys imagebuilder:CreatedResourceTag/<key> imagebuilder:Ec2MetadataHttpTokens imagebuilder:StatusTopicArn	iam:PassRole sns:Publish
UpdateLifecyclePolicy	授予更新现有生命周期策略的权限	写入	lifecyclePolicy*	imagebuilder:LifecyclePolicyResourceType	iam:PassRole

由 Amazon EC2 Image Builder 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从

而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
component	arn:${Partition}:imagebuilder:${Region}:${Account}:component/${ComponentName}/${ComponentVersion}/${ComponentBuildVersion}	aws:ResourceTag/${TagKey}
componentVersion	arn:${Partition}:imagebuilder:${Region}:${Account}:component/${ComponentName}/${ComponentVersion}	aws:ResourceTag/${TagKey}
distributionConfiguration	arn:${Partition}:imagebuilder:${Region}:${Account}:distribution-configuration/${DistributionConfigurationName}	aws:ResourceTag/${TagKey}
image	arn:${Partition}:imagebuilder:${Region}:${Account}:image/${ImageName}/${ImageVersion}/${ImageBuildVersion}	aws:ResourceTag/${TagKey}
imageVersion	arn:${Partition}:imagebuilder:${Region}:${Account}:image/${ImageName}/${ImageVersion}	aws:ResourceTag/${TagKey}
imageRecipe	arn:${Partition}:imagebuilder:${Region}:${Account}:image-recipe/${ImageRecipeName}/${ImageRecipeVersion}	aws:ResourceTag/${TagKey}
containerRecipe	arn:${Partition}:imagebuilder:${Region}:${Account}:container-recipe/${ContainerRecipeName}/${ContainerRecipeVersion}	aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
imagePipeline	arn:${Partition}:imagebuilder:${Region}:${Account}:image-pipeline/${ImagePipelineName}	aws:ResourceTag/${TagKey}
infrastructureConfiguration	arn:${Partition}:imagebuilder:${Region}:${Account}:infrastructure-configuration/${ResourceId}	aws:ResourceTag/${TagKey}
kmsKey	arn:${Partition}:kms:${Region}:${Account}:key/${KeyId}	
lifecycleExecution	arn:${Partition}:imagebuilder:${Region}:${Account}:lifecycle-execution/${LifecycleExecutionId}	
lifecyclePolicy	arn:${Partition}:imagebuilder:${Region}:${Account}:lifecycle-policy/${LifecyclePolicyName}	aws:ResourceTag/${TagKey}
workflow	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow/${WorkflowType}/${WorkflowName}/${WorkflowVersion}/${WorkflowBuildVersion}	aws:ResourceTag/${TagKey}
workflowVersion	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow/${WorkflowType}/${WorkflowName}/${WorkflowVersion}	aws:ResourceTag/${TagKey}
workflowExecution	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow-execution/${WorkflowExecutionId}	
workflowStepExecution	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow-step-execution/${WorkflowStepExecutionId}	

Amazon EC2 Image Builder 的条件密钥

Amazon I EC2 mage Builder 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对来筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按附加到资源的标签键值对筛选操作	字符串
aws:TagKeys	根据在请求中是否具有标签键来筛选访问	ArrayOfString
imagebuilder:CreatedResourceTag/<key>	根据附加到 Image Builder 所创建的资源的标签键值对来筛选访问	字符串
imagebuilder:CreatedResourceTagKeys	根据在请求中是否具有标签键来筛选访问	ArrayOfString
imagebuilder:Ec2MetadataHttpTokens	根据请求中指定的 EC2 实例元数据 HTTP 令牌要求筛选访问权限	字符串
imagebuilder:LifecyclePolicyResourceType	按请求中指定的生命周期策略资源类型筛选访问权限	字符串

条件键	描述	类型
imagebuilder:StatusTopicArn	按将发送终端状态通知的请求中的 SNS Topic Arn 筛选访问权限	ARN

Amazon EC2 Instance Connect 的操作、资源和条件密钥

Ama EC2 zon Instance Connect（服务前缀:ec2-instance-connect）提供以下特定于服务的资源、操作和条件上下文密钥以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Instance Connec EC2 t 定义的操作
- 由 Amazon Instance Connect EC2 定义的资源类型
- Amazon EC2 实例 Connect 的条件密钥

Amazon Instance Connec EC2 t 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
OpenTunnel	授予使用 EC2 Instance Connect 终端节点与 EC2 实例建立 SSH 连接的权限	写入	instance-connect-endpoint*		
			instance-connect-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2-instance-connect:remotePort ec2-instance-connect:privat	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				elpAddress ec2-instance-connect:MaxTunnelDuration	
SendSSHPublicKey	授予将 SSH 公钥推送到指定 EC2 实例以用于标准 SSH 的权限	写入	instance*		
				ec2:osuser	
SendSerialConsoleSSHPublicKey	授予将 SSH 公钥推送到指定 EC2 实例以用于串行控制台 SSH 的权限	写入	instance*		

由 Amazon Instance Connect EC2 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
instance	`arn:${Partition}:ec2:${Region}:${Account}:instance/${InstanceId}`	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}

资源类型	ARN	条件键
instance-connect-endpoint	arn:${Partition}:ec2:${Region}:${Account}:instance-connect-endpoint/${InstanceConnectEndpointId}	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}

Amazon EC2 实例 Connect 的条件密钥

Ama EC2 zon Instance Connect 定义了以下条件密钥，这些条件键可用于 IAM 策略的Condition元素中。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
ec2-instance-connect:maxTunnelDuration	按与实例关联的最大会话持续时间筛选访问权限	数值
ec2-instance-connect:privateIpAddress	按与实例关联的私有 IP 地址筛选访问权限	IPAddress
ec2-instance-connect:remotePort	按与实例关联的端口号筛选访问权限	数值
ec2:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串

条件键	描述	类型
ec2:osuser	通过指定用于启动实例的 AMI 的默认用户名来筛选访问	字符串

Amazon EKS Auth 的操作、资源和条件键

Amazon EKS Auth（服务前缀：eks-auth）提供了以下可在 IAM 权限策略中使用的服务特定资源、操作和条件上下文键。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon EKS Auth 定义的操作
- Amazon EKS Auth 定义的资源类型
- Amazon EKS Auth 的条件键

Amazon EKS Auth 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssumeRoleForPodIdentity	授予将 Kubernetes 服务账号令牌交换为临时证书的权限 Amazon	读取	cluster*		

Amazon EKS Auth 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
cluster	`arn:${Partition}:eks:${Region}:${Account}:cluster/${ClusterName}`	aws:ResourceTag/${TagKey}

Amazon EKS Auth 的条件键

Amazon EKS Auth 定义了以下可以在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:ResourceTag/${TagKey}	按标签键值对筛选访问	字符串

Amazon Elastic Beanstalk 的操作、资源和条件键

Amazon Elastic Beanstalk（服务elasticbeanstalk前缀:）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon Elastic Beanstalk 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AbortEnvironmentUpdate	授予权限以取消正在进行的环境配置更新或应用程序版本部署	写入	environment*	elasticbeanstalk:InApplication	
AddTags	授予权限以将标签添加到 Elastic Beanstalk 资源并更新标签值	标记	application		
			applicationversion		
			configurationtemplate		
			environment		
			platform		
				aws:RequestTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys	
ApplyEnvironmentManagedAction	授予权限以立即应用计划的托管操作	写入	environment*	elasticbeanstalk:InApplication	
AssociateEnvironmentOperationsRole	授予权限以将操作角色与环境关联	写入	environment*		
CheckDNSAvailability	授予权限以检查别名记录可用性	读取			
ComposeEnvironments	授予权限以创建或更新一组环境，每个环境运行单个应用程序的单独组件	写入	application*		
			applicationversion*	elasticbeanstalk:InApplication	
CreateApplication	授予权限以创建新的应用程序	写入	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateApplicationVersion	授予权限以便为应用程序创建应用程序版本	写入	application*		
			applicationversion*	elasticbeanstalk:InApplication aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfigurationTemplate	授予权限以创建配置模板	写入	configurationtemplate*	elasticbeanstalk:InApplication	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				elasticbeanstalk:FromApplication elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromEnvironment elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironment	授予权限以便为应用程序启动环境	写入	environment*	elasticbeanstalk:InApplication	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform aws:RequestTag/${TagKey} aws:TagKeys	
CreatePlatformVersion	授予权限以创建自定义平台的新版本	写入	platform*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStorageLocation	授予权限以便为账户创建 Amazon S3 存储位置	写入			
DeleteApplication	授予权限以删除应用程序以及所有关联的版本和配置	写入	application*		
DeleteApplicationVersion	授予权限以从应用程序中删除应用程序版本	写入	applicationversion*	elasticbeanstalk:InApplication	
DeleteConfigurationTemplate	授予权限以删除配置模板	写入	configurationtemplate*	elasticbeanstalk:InApplication	
DeleteEnvironmentConfiguration	授予权限以删除与运行的环境关联的草稿配置	写入	environment*	elasticbeanstalk:InApplication	
DeletePlatformVersion	授予权限以删除自定义平台的版本	写入	platform*		
DescribeAccountAttributes	授予权限以检索账户属性列表，包括资源配额	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeApplicationVersions	授予检索存储在 Elasti Amazon c Beanstalk 存储桶中的应用程序版本列表的权限	列表	applicationversion	elasticbeanstalk:InApplication	
DescribeApplications	授予权限以检索现有应用程序的描述	列表	application		
DescribeConfigurationOptions	授予权限以检索环境配置选项描述	读取	configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	
			solutionstack		
DescribeConfigurationSettings	授予权限以检索配置集设置描述	读取	configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	
DescribeEnvironmentHealth	授予权限以检索有关环境总体运行状况的信息	读取	environment		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeEnvironmentManagedActionHistory	授予权限以检索环境的完成和失败托管操作列表	读取	environment	elasticbeanstalk:InApplication	
DescribeEnvironmentManagedActions	授予权限以检索环境即将执行和正在执行的托管操作列表	读取	environment	elasticbeanstalk:InApplication	
DescribeEnvironmentResources	授予检索环境 Amazon 资源列表的权限	读取	environment	elasticbeanstalk:InApplication	
DescribeEnvironments	授予权限以检索现有环境的描述	列表	environment	elasticbeanstalk:InApplication	
DescribeEvents	授予权限以检索与一组条件匹配的事件描述列表	读取	application		
			applicationversion	elasticbeanstalk:InApplication	
			configurationtemplate	elasticbeanstalk:InApplication	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			environment	elasticbeanstalk:InApplication	
DescribeInstancesHealth	授予权限以检索有关环境实例运行状况的更多详细信息	读取	environment		
DescribePlatformVersion	授予权限以检索托管平台版本描述	读取	platform		
DisassociateEnvironmentOperationsRole	授予权限以取消操作角色与环境的关联	写入	environment*		
ListAvailableSolutionStacks	授予权限以检索可用的解决方案堆栈名称列表	列表	solutionstack		
ListPlatformBranches	授予权限以检索可用平台分支列表	列表			
ListPlatformVersions	授予权限以检索可用的平台列表	列表	platform		
ListTagsForResource	授予权限以检索 Elastic Beanstalk 资源的标签列表	读取	application		
			applicationversion		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			configurationtemplate		
			environment		
			platform		
PutInstanceStatistics	授予权限以提交实例统计数据来改进运行状况	写入	application*		
			environment*		
RebuildEnvironment	授予删除和重新创建环境的所有 Amazon 资源以及强制重启的权限	写入	environment*	elasticbeanstalk:InApplication	
RemoveTags	授予权限以从 Elastic Beanstalk 资源中删除标签	标记	application		
			applicationversion		
			configurationtemplate		
			environment		
			platform		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys	
RequestEnvironmentInfo	授予权限以启动编译部署的环境信息的请求	读取	environment*	elasticbeanstalk:InApplication	
RestartAppServer	授予请求环境以重启在每个 Amazon EC2 实例上运行的应用程序容器服务器的权限	写入	environment*	elasticbeanstalk:InApplication	
RetrieveEnvironmentInfo	授予从 RequestEnvironmentInfo 请求中检索已编译信息的权限	读取	environment*	elasticbeanstalk:InApplication	
SwapEnvironmentCNAMEs	授予交换两个环境 CNAMEs 的权限	写入	environment*	elasticbeanstalk:InApplication	
				elasticbeanstalk:FromEnvironment	
TerminateEnvironment	授予权限以终止环境	写入	environment*	elasticbeanstalk:InApplication	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateApplication	授予权限以使用指定的属性更新应用程序	写入	application*		
UpdateApplicationResourceLifecycle	授予权限以更新与应用程序关联的应用程序版本生命周期策略	写入	application*		
UpdateApplicationVersion	授予权限以使用指定的属性更新应用程序版本	写入	applicationversion*	elasticbeanstalk:InApplication	
UpdateConfigurationTemplate	授予权限以使用指定的属性或配置选项值更新配置模板	写入	configurationtemplate*	elasticbeanstalk:InApplication	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				elasticbeanstalk:FromApplication elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromEnvironment elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateEnvironment	授予更新环境的权限	写入	environment*	elasticbeanstalk:InApplication	
				elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform	
UpdateTagsForResource	不授予更新标签的权限。要授予向 Elastic Beanstalk 资源添加标签、移除标签和更新标签值的权限，请指定 elasticbeanstalk: 和 elasticbeanstalk: 和 elasticbeanstalk：AddTags RemoveTags	标记	application		
			applicationversion		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			configurationtemplate		
			environment		
			platform		
				aws:RequestTag/${TagKey} aws:TagKeys	
ValidateConfigurationSettings	授予权限以检查配置模板或环境的一组配置设置的有效性	读取	configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	

Amazon Elastic Beanstalk 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}	
platform	arn:${Partition}:elasticbeanstalk:${Region}::platform/${PlatformNameWithVersion}	

Amazon Elastic Beanstalk 的条件键

Amazon Elastic Beanstalk 定义了以下可以在 IAM 策略元素Condition中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对以筛选操作	字符串
aws:ResourceTag/${TagKey}	根据附加到资源的标签键值对筛选操作	字符串
aws:TagKeys	根据在请求中是否具有标签键以筛选操作	ArrayOfString
elasticbeanstalk:FromApplication	将应用程序作为输入参数的依赖项或限制以筛选访问	ARN
elasticbeanstalk:FromApplicationVersion	将应用程序版本作为输入参数的依赖项或限制以筛选访问	ARN
elasticbeanstalk:FromConfigurationTemplate	将配置模板作为输入参数的依赖项或限制以筛选访问	ARN
elasticbeanstalk:FromEnvironment	将环境作为输入参数的依赖项或限制以筛选访问	ARN
elasticbeanstalk:FromPlatform	将平台作为输入参数的依赖项或限制以筛选访问	ARN
elasticbeanstalk:FromSolutionStack	将解决方案堆栈作为输入参数的依赖项或限制以筛选访问	ARN

条件键	描述	类型
elasticbeanstalk:InApplication	按包含运行操作的资源的应用程序筛选访问	ARN

Amazon Elastic Block Store 的操作、资源和条件键

Amazon Elastic Block Store（服务前缀：ebs）提供可在 IAM 权限策略中使用的以下服务特定资源、操作和条件上下文键。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Elastic Block Store 定义的操作
- Amazon Elastic Block Store 定义的资源类型
- Amazon Elastic Block Store 的条件键

Amazon Elastic Block Store 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CompleteSnapshot	授予权限以在将所有必需的数据块写入快照后密封和完成快照	写入	snapshot*		
				aws:ResourceTag/${TagKey}	
GetSnapshotBlock	授予权限以在 Amazon Elastic Block Store (EBS) 快照中返回块数据	Read	snapshot*		
				aws:ResourceTag/${TagKey}	
ListChangedBlocks	授予权限以列出相同卷/快照谱系的两个 Amazon Elastic Block Store (EBS) 快照之间不同的数据块	读取	snapshot*		
				aws:ResourceTag/${TagKey}	
ListSnapshotBlocks	授予权限以列出 Amazon Elastic Block Store (EBS) 快照中的数据块	读取	snapshot*		
				aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutSnapshotBlock	授予向 StartSnapshot 操作创建的快照写入数据块的权限	写入	snapshot*		
				aws:ResourceTag/${TagKey}	
StartSnapshot	授予权限以创建新的 EBS 快照	写入	snapshot		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ebs:Description ebs:ParentSnapshot ebs:VolumeSize	

Amazon Elastic Block Store 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
snapshot	arn:${Partition}:ec2:${Region}::snapshot/${SnapshotId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ebs:Description ebs:ParentSnapshot ebs:VolumeSize

Amazon Elastic Block Store 的条件键

Amazon Elastic Block Store 定义以下可以在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中允许的标签键值对筛选访问	字符串
aws:ResourceTag/${TagKey}	按某个资源的标签键值对筛选访问	字符串
aws:TagKeys	按请求中允许的标签键列表筛选访问	ArrayOfString
ebs:Description	根据正在创建的快照的描述筛选访问	字符串
ebs:ParentSnapshot	按父快照的 ID 筛选访问	字符串

条件键	描述	类型
ebs:VolumeSize	按正在创建的快照的卷的大小（以 GiB 为单位）筛选访问	数值

Amazon Elastic Container Registry 的操作、资源和条件键

Amazon Elastic Container Registry（服务前缀：ecr）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Elastic Container Registry 定义的操作
- Amazon Elastic Container Registry 定义的资源类型
- Amazon Elastic Container Registry 的条件键

Amazon Elastic Container Registry 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchCheckLayerAvailability	授予权限以检查指定注册表和存储库中多个图像图层的可用性	Read	repository*		
BatchDeleteImage	授予权限以删除指定存储库中的指定图像列表	Write	repository*		
BatchGetImage	授予权限以获取指定存储库中指定图像的详细信息	读取	repository*		
BatchGetRepositoryScanningConfiguration	授予权限以检索存储库列表的存储库扫描配置	读取	repository*		
BatchImportUpstreamImage[仅权限]	授予权限以从上游注册表检索镜像并将其导入到您的私有注册表	写入			
CompleteLayerUpload	授予权限以通知 Amazon ECR 用于指定注册表、存储库名称和上传 ID 的图像图层上传已完成	写入	repository*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreatePullThroughCacheRule	授予创建新的推送缓存规则的权限	写入			iam:CreateServiceLinkedRole
CreateRepository	授予权限以创建图像存储库	写入	repository*		ecr:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRepositoryCreationTemplate	授予创建存储库创建模板的权限	写入			ecr:CreateRepository ecr:PutLifecyclePolicy ecr:SetRepositoryPolicy iam:CreateServiceLinkedRole iam:PassRole
DeleteLifecyclePolicy	授予权限以删除指定的生命周期策略	写入	repository*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeletePullThroughCacheRule	授予删除推送缓存规则的权限	写入			
DeleteRegistryPolicy	授予删除注册表策略的权限	权限管理			
DeleteRepository	授予权限以删除现有图像存储库	写入	repository*		
DeleteRepositoryCreationTemplate	授予删除存储库创建模板的权限	写入			
DeleteRepositoryPolicy	授予权限以从指定存储库中删除存储库策略	权限管理	repository*		
DescribeImageReplicationStatus	授予权限以检索注册表中的镜像的复制状态，包括复制失败时的失败原因	读取	repository*		
DescribeImageScanFindings	授予权限以描述指定图像的图像扫描结果	Read	repository*		
DescribeImages	授予权限以获取有关存储库中图像的元数据，包括图像大小、图像标签和创建日期	列表	repository*		
DescribePullThroughCacheRules	授予描述推送缓存规则的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeRegistry	授予权限以描述注册表设置	Read			
DescribeRepositories	授予权限以描述注册表中的图像存储库	读取	repository*		
DescribeRepositoryCreationTemplates	授予描述存储库创建模板的权限	读取			
GetAccountSetting	授予权限以检索账户设置	读取		ecr:AccountSetting	
GetAuthorizationToken	授予权限以检索 12 小时内对指定注册表有效的令牌	Read			
GetDownloadUrlForLayer	授予权限以检索与图像图层对应的下载 URL	读取	repository*		
GetImageCopyStatus[仅权限]	授予检索图像副本状态的权限	读取			
GetLifecyclePolicy	授予权限以检索指定的生命周期策略	Read	repository*		
GetLifecyclePolicyPreview	授予权限以检索指定的生命周期策略预览请求的结果	Read	repository*		
GetRegistryPolicy	授予检索注册表策略的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetRegistryScanningConfiguration	授予权限以检索注册表扫描配置	读取			
GetRepositoryPolicy	授予权限以检索指定存储库的存储库策略	Read	repository*		
InitiateLayerUpload	授予权限以通知 Amazon ECR 您打算上传图像图层	写入	repository*		
ListImages	授予列出给定仓库所有图像 IDs 的权限	列表	repository*		
ListTagsForResource	授予权限以列出 Amazon ECR 资源标签	读取	repository*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutAccountSetting	授予权限以更新账户设置	写入		ecr:AccountSetting	
PutImage	授予权限以创建或更新与图像关联的图像清单	Write	repository*		
PutImageScanningConfiguration	授予权限以更新存储库的图像扫描配置	Write	repository*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutImageTagMutability	授予权限以更新存储库的图像标签可变性设置	Write	repository*		
PutLifecyclePolicy	授予权限以创建或更新生命周期策略	Write	repository*		
PutRegistryPolicy	授予更新注册表策略的权限	权限管理			
PutRegistryScanningConfiguration	授予权限以更新注册表扫描配置	写入			
PutReplicationConfiguration	授予更新注册表的复制配置的权限	写入			iam:CreateServiceLinkedRole
ReplicateImage[仅权限]	授予将映像复制到目标注册表的权限	Write	repository*		
SetRepositoryPolicy	授予权限以在指定存储库上应用存储库策略来控制访问权限	Permissions management	repository*		
StartImageScan	授予权限以启动图像扫描	Write	repository*		
StartLifecyclePolicyPreview	授予权限以启动指定生命周期策略的预览	Write	repository*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
TagResource	授予权限以标记 Amazon ECR 资源	Tagging	repository*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予权限以取消标记 Amazon ECR 资源	标记	repository*		
				aws:TagKeys	
UpdatePullThroughCacheRule	授予更新直通式缓存规则的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateRepositoryCreationTemplate	授予权限以更新存储库创建模板	写入			ecr:CreateRepository ecr:PutLifecyclePolicy ecr:SetRepositoryPolicy iam:CreateServiceLinkedRole iam:PassRole
UploadLayerPart	授予权限以将图像图层部分上传到 Amazon ECR	写入	repository*		
ValidatePullThroughCacheRule	授予验证直通式缓存规则的权限	读取			

Amazon Elastic Container Registry 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
repository	arn:${Partition}:ecr:${Region}:${Account}:repository/${RepositoryName}	aws:ResourceTag/${TagKey} ecr:ResourceTag/${TagKey}

Amazon Elastic Container Registry 的条件键

Amazon Elastic Container Registry 定义以下可以在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按每个标签的允许值集筛选访问	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签值筛选访问权限	字符串
aws:TagKeys	按请求中是否具有必需标签来筛选访问	ArrayOfString
ecr:AccountSetting	按 ECR 账户设置名称筛选访问权限	字符串
ecr:ResourceTag/${TagKey}	按与资源关联的标签值筛选访问权限	字符串

Amazon Elastic File System 的操作、资源和条件键

Amazon Elastic File System（服务前缀：elasticfilesystem）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon Elastic File System 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
Backup[仅权限]	授予为现有文件系统启动备份作业的权限	Write	file-system*		
ClientMount[仅权限]	授予允许 NFS 客户端对文件系统进行读取访问的权限	Read	file-system*		
				elasticfilesystem:AccessPointArn elasticfilesystem:AccessedViaMountTarget	
ClientRootAccess[仅权限]	授予允许 NFS 客户端对文件系统进行根访问的权限	Write	file-system*		
				elasticfilesystem:AccessPointArn elasticfilesystem:AccessedViaMountTarget	
ClientWrite[仅权限]	授予允许 NFS 客户端对文件系统进行写入访问的权限	Write	file-system*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				elasticfilesystem:AccessPointArn elasticfilesystem:AccessedViaMountTarget	
CreateAccessPoint	授予为指定文件系统创建访问点的权限	Write	file-system*		elasticfilesystem:TagResource
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateFileSystem	授予创建新的空文件系统的权限	Write		aws:RequestTag/${TagKey} aws:TagKeys elasticfilesystem:Encrypted	elasticfilesystem:TagResource

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateMountTarget	授予为文件系统创建挂载目标的权限	写入	file-system*		
CreateReplicationConfiguration	授予权限以创建新的复制配置	写入	file-system*		
CreateTags	授予创建或覆盖与文件系统关联的标签的权限；已弃用，请参阅 TagResource	标记	file-system*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessPoint	授予删除指定访问点的权限	Write	access-point*		
DeleteFileSystem	授予删除文件系统的权限，永久终止访问其内容	Write	file-system*		
DeleteFileSystemPolicy	授予权限以删除文件系统的资源级策略	权限管理	file-system*		
DeleteMountTarget	授予权限以删除指定挂载目标	写入	file-system*		
DeleteReplicationConfiguration	授予权限以删除复制配置	写入	file-system*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteTags	授予从文件系统中删除指定标签的权限；已弃用，请参阅 UntagResource	标记	file-system*		
				aws:TagKeys	
DescribeAccessPoints	授予查看 Amazon EFS 接入点描述的权限	List	access-point		
			file-system		
DescribeAccountPreferences	授予查看对账户有效的账户首选项的权限	列表			
DescribeBackupPolicy	授予查看 Amazon EFS 文件系统 BackupPolicy 对象的权限	读取	file-system*		
DescribeFileSystemPolicy	授予查看 Amazon EFS 文件系统的资源级策略的权限	读取	file-system		
DescribeFileSystems	授予权限以查看由文件系统指定的 Amazon EFS 文件系统的描述 CreationToken 或 FileSystemId；或查看调用方 Amazon Web Services 账户 在被调用的终端节点 Amazon 所在区域内拥有的所有文件系统的描述	列表	file-system		
DescribeLifecycleConfiguration	授予查看 Amazon EFS 文件系统 LifecycleConfiguration 对象的权限	读取	file-system*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeMountTargetSecurityGroups	授予查看挂载目标的有效安全组的权限	Read	file-system*		
DescribeMountTargets	授予查看文件系统所有或特定挂载目标的描述的权限	读取	file-system*		
			access-point		
DescribeReplicationConfigurations	授予权限以查看由指定的 Amazon EFS 复制配置的描述 FileSystemId；或查看调用者 Amazon Web Services 账户 在被调用的终端节点 Amazon 所在区域内拥有的所有复制配置的描述	列表	file-system		
DescribeTags	授予查看与文件系统关联的标签的权限	Read	file-system*		
ListTagsForResource	授予查看与指定 Amazon EFS 资源关联的标签的权限	Read	access-point		
			file-system		
ModifyMountTargetSecurityGroups	授予修改挂载目标的一组有效安全组的权限	Write	file-system*		
PutAccountPreferences	授予设置账户的账户首选项的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutBackupPolicy	授予通过创建新 BackupPolicy 对象启用或禁用 Backup 自动 Amazon 备份的权限	写入	file-system*		
PutFileSystemPolicy	授予权限以应用资源级策略，该策略定义了指定文件系统中给定参与者允许或拒绝的操作	权限管理	file-system*		
PutLifecycleConfiguration	通过创建新 LifecycleConfiguration 对象授予启用生命周期管理的权限	写入	file-system*		
ReplicationRead[仅权限]	授予读取文件系统数据以进行复制的权限	读取	file-system*		
ReplicationWrite[仅权限]	授予将数据复制到文件系统的权限	写入	file-system*		
Restore[仅权限]	授予启动文件系统备份的还原作业的权限	Write	file-system*		
TagResource	授予创建或覆盖与指定 Amazon EFS 资源关联的标签的权限	Tagging	access-point		
			file-system		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys elasticfilesystem:CreateAction	
UntagResource	授予从 Amazon EFS 资源删除指定标签的权限	Tagging	access-point		
			file-system		
				aws:TagKeys	
UpdateFileSystem	授予更新现有文件系统的吞吐量模式或预置吞吐量的权限	写入	file-system*		
UpdateFileSystemProtection	授予更新现有文件系统的文件系统保护的权限	写入	file-system*		

Amazon Elastic File System 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
file-system	arn:${Partition}:elasticfilesystem:${Region}:${Account}:file-system/${FileSystemId}	aws:ResourceTag/${TagKey}
access-point	arn:${Partition}:elasticfilesystem:${Region}:${Account}:access-point/${AccessPointId}	aws:ResourceTag/${TagKey}

Amazon Elastic File System 的条件键

Amazon Elastic File System 定义以下可以在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中允许的标签键值对筛选访问	字符串
aws:ResourceTag/${TagKey}	按某个资源的标签键值对筛选访问	字符串
aws:TagKeys	按请求中允许的标签键列表筛选访问	ArrayOfString
elasticfilesystem:AccessPointArn	按用于挂载文件系统的访问点的 ARN 筛选访问	ARN
elasticfilesystem:AccessedViaMountTarget	按是否通过挂载目标访问文件系统筛选访问	布尔型

条件键	描述	类型
elasticfilesystem:CreateAction	按资源创建 API 操作的名称筛选访问	字符串
elasticfilesystem:Encrypted	按用户是否只能创建加密还是未加密的文件系统来筛选访问	布尔型

Amazon Elastic Kubernetes Service 的操作、资源和条件键

Amazon Elastic Kubernetes Service（服务前缀：eks）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Elastic Kubernetes Service 定义的操作
- Amazon Elastic Kubernetes Service 定义的资源类型
- Amazon Elastic Kubernetes Service 的条件键

Amazon Elastic Kubernetes Service 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用

Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AccessKubernetesApi[仅权限]	授予通过 EKS 控制台查看 Kubernetes 对象的权限 Amazon	读取	cluster*		
AssociateAccessPolicy	授予将 Amazon EKS 访问策略与 Amazon EKS 访问条目关联的权限	写入	access-entry*		
				eks:policyArn eks:namespaces eks:accessScope	
AssociateEncryptionConfig	授予权限以将加密配置关联到集群	Write	cluster*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateIdentityProviderConfig	授予权限以将身份提供商配置关联到集群	写入	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys eks:clientId eks:issuerUrl	
CreateAccessEntry	授予创建 Amazon EKS 访问条目的权限	写入	cluster*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys eks:principalArn eks:kubernetesGroups eks:username eks:accessEntryType	
CreateAddon	授予权限以创建 Amazon EKS 附加组件	Write	cluster*		
			podidentityassociation		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateCluster	授予权限以创建 Amazon EKS 集群	写入		aws:RequestTag/${TagKey} aws:TagKeys eks:bootstrapClusterCreatorAdminPermissions eks:bootstrapSelfManagedAddons eks:authenticationMode eks:supportType eks:computeConfigEnabled eks:elasticLoadBalancingEnabled	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				eks:blockStorageEnabled	
CreateEksAnywhereSubscription	授予创建 EKS Anywhere 订阅的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFargateProfile	授予创建 Amazon Fargate 个人资料的权限	写入	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNodegroup	授予权限以创建 Amazon EKS 节点组	写入	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePodIdentityAssociation	授予创建 EKS 容器组身份关联的权限	写入	cluster*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessEntry	授予删除 Amazon EKS 访问条目的权限	写入	access-entry*		
DeleteAddon	授予权限以删除 Amazon EKS 附加组件	Write	addon*		
			podidentityassociation		
DeleteCluster	授予权限以删除 Amazon EKS 集群	写入	cluster*		
DeleteEksAnywhereSubscription	授予描述 EKS Anywhere 订阅的权限	写入	eks-anywhere-subscription*		
DeleteFargateProfile	授予删除 Amazon Fargate 个人资料的权限	写入	fargateprofile*		
DeleteNodegroup	授予权限以删除 Amazon EKS 节点组	写入	nodegroup*		
DeletePodIdentityAssociation	授予删除 EKS 容器组身份关联的权限	写入	podidentityassociation*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeregisterCluster	授予取消注册外部集群的权限	写入	cluster*		
DescribeAccessEntry	授予描述 Amazon EKS 访问条目的权限	读取	access-entry*		
DescribeAddon	授予权限以检索有关 Amazon EKS 附加组件的描述性信息	读取	addon*		
DescribeAddonConfiguration	授予列出有关 Amazon EKS 附加组件的配置选项的权限	读取			
DescribeAddonVersions	授予权限以检索有关 Amazon EKS Add-ons 支持的附加组件的描述性版本信息	Read			
DescribeCluster	授予权限以检索有关 Amazon EKS 集群的描述性信息	读取	cluster*		
DescribeClusterVersions	授予权限以检索有关 Amazon EKS 集群支持的 Kubernetes 版本的描述性信息	读取			
DescribeEksAnywhereSubscription	授予描述 EKS Anywhere 订阅的权限	读取	eks-anywhere-subscription*		
DescribeFargateProfile	授予检索与集群关联的 Far Amazon gate 配置文件的描述性信息的权限	读取	fargateprofile*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeIdentityProviderConfig	授予权限以检索与集群关联的 Idp config 的相关描述性信息	读取	identityproviderconfig*		
DescribeInsight	授予检索指定集群中检测到的见解的描述性信息的权限	读取	cluster*		
DescribeNodegroup	授予权限以检索有关 Amazon EKS 节点组的描述性信息	读取	nodegroup*		
DescribePodIdentityAssociation	授予描述 EKS 容器组身份关联的权限	读取	podidentityassociation*		
DescribeUpdate	授予权限以检索给定 Amazon EKS cluster/nodegroup/add 的给定更新（在指定或默认区域）	读取	cluster*		
			addon		
			nodegroup		
DisassociateAccessPolicy	授予将 Amazon EKS 访问策略与 Amazon EKS 访问条目取消关联的权限	写入	access-entry*		
				eks:policyArn eks:namespaces eks:accessScope	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DisassociateIdentityProviderConfig	授予权限以删除关联的 Idp config	写入	identityproviderconfig*		
ListAccessEntries	授予列出所有 Amazon EKS 访问条目的权限	列表	cluster*		
ListAccessPolicies	授予列出 Amazon EKS 访问策略的权限	列表			
ListAddons	授予在您的 Amazon Web Services 账户（指定或默认区域）列出给定集群的 Amazon EKS 插件的权限	列表	cluster*		
ListAssociatedAccessPolicies	授予列出关联访问策略与 Amazon EKS 访问条目的权限	列表	access-entry*		
ListClusters	授予列出您的 Amazon Web Services 账户（指定或默认区域）中的 Amazon EKS 集群的权限	列表			
ListEksAnywhereSubscriptions	授予列出 EKS Anywhere 订阅的权限	列表			
ListFargateProfiles	授予列出您 Amazon Web Services 账户（在指定或默认区域）中与给定集群关联的 Amazon Fargate 配置文件的权限	列表	cluster*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListIdentityProviderConfigs	授予列出您 Amazon Web Services 账户（在指定或默认区域）中与给定集群关联的 Idp 配置的权限	列表	cluster*		
ListInsights	授予列出指定集群的所有检测见解的权限	列表	cluster*		
ListNodegroups	授予权限以列出您的 Amazon Web Services 账户（在指定或默认区域）连接到给定集群的 Amazon EKS 节点组	列表	cluster*		
ListPodIdentityAssociations	授予列出 EKS 容器组身份关联的权限	列表	cluster*		
ListTagsForResource	授予列出指定资源的标签的权限	读取	addon		
			cluster		
			eks-anywhere-subscription		
			fargateprofile		
			identityproviderconfig		
			nodegroup		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListUpdates	授予列出给定 Amazon EKS cluster/nodegroup/add 更新的权限（在指定或默认区域）	列表	cluster*		
			addon		
			nodegroup		
RegisterCluster	授予注册外部集群的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	授予标记指定资源的权限	Tagging	access-entry		
			addon		
			cluster		
			eks-anywhere-subscription		
			fargateprofile		
			identityproviderconfig		
			nodegroup		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			podidentityassociation		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予取消标记指定资源的权限	标记	access-entry		
			addon		
			cluster		
			eks-anywhere-subscription		
			fargateprofile		
			identityproviderconfig		
			nodegroup		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			podidentityassociation		
				aws:TagKeys	
UpdateAccessEntry	授予更新 Amazon EKS 访问条目的权限	写入	access-entry*		
UpdateAddon	授予权限以更新 Amazon EKS 附加组件配置，例如 VPC-CNI 版本	Write	addon*		
			podidentityassociation		
UpdateClusterConfig	授予权限以更新 Amazon EKS 集群配置（例如，API 服务器终端节点访问）	Write	cluster*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				eks:authenticationMode eks:supportType eks:computeConfigEnabled eks:elasticLoadBalancingEnabled eks:blockStorageEnabled	
UpdateClusterVersion	授予权限以更新 Amazon EKS 集群的 Kubernetes 版本	写入	cluster*		
UpdateEksAnywhereSubscription	授予更新 EKS Anywhere 订阅的权限	写入	eks-anywhere-subscription*		
UpdateNodegroupConfig	授予更新 Amazon EKS 节点组配置（例如：min/max/desired 容量或标签）的权限	写入	nodegroup*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateNodegroupVersion	授予权限以更新 Amazon EKS 节点组的 Kubernetes 版本	写入	nodegroup*		
UpdatePodIdentityAssociation	授予更新 EKS 容器组身份关联的权限	写入	podidentityassociation*		

Amazon Elastic Kubernetes Service 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
cluster	arn:${Partition}:eks:${Region}:${Account}:cluster/${ClusterName}	aws:ResourceTag/${TagKey}
nodegroup	arn:${Partition}:eks:${Region}:${Account}:nodegroup/${ClusterName}/${NodegroupName}/${UUID}	aws:ResourceTag/${TagKey}
addon	arn:${Partition}:eks:${Region}:${Account}:addon/${ClusterName}/${AddonName}/${UUID}	aws:ResourceTag/${TagKey}
fargateprofile	arn:${Partition}:eks:${Region}:${Account}:fargateprofile/${ClusterName}/${FargateProfileName}/${UUID}	aws:ResourceTag/${TagKey}
identityproviderconfig	arn:${Partition}:eks:${Region}:${Account}:identityproviderconfig/${Clust	aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
	erName}/${IdentityProviderType}/${IdentityProviderConfigName}/${UUID}	
eks-anywhere-subscription	arn:${Partition}:eks:${Region}:${Account}:eks-anywhere-subscription/${UUID}	aws:ResourceTag/${TagKey}
podidentityassociation	arn:${Partition}:eks:${Region}:${Account}:podidentityassociation/${ClusterName}/${UUID}	aws:ResourceTag/${TagKey}
access-entry	arn:${Partition}:eks:${Region}:${Account}:access-entry/${ClusterName}/${IamIdentityType}/${IamIdentityAccountID}/${IamIdentityName}/${UUID}	aws:ResourceTag/${TagKey} eks:accessEntryType eks:clusterName eks:kubernetesGroups eks:principalArn eks:username
access-policy	arn:${Partition}:eks::aws:cluster-access-policy/${AccessPolicyName}	

Amazon Elastic Kubernetes Service 的条件键

Amazon Elastic Kubernetes Service 定义以下可以在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按用户向 EKS 服务发出的请求中包含的键筛选访问	字符串
aws:ResourceTag/${TagKey}	按标签键值对筛选访问	字符串
aws:TagKeys	按用户向 EKS 服务发出的请求中包含的所有标签键名称的列表筛选访问	ArrayOfString
eks:accessEntryType	按用户向 EKS 服务发出的访问条目请求中所包含的访问条目类型筛选访问权限	字符串
eks:accessScope	按用户向 EKS 服务发出的关联/取消关联访问策略请求中包含的 accessScope 筛选访问权限	字符串
eks:authenticationMode	按创建/更新集群请求中所包含的身份验证模式筛选访问权限	字符串
eks:blockStorageEnabled	在创建/更新集群请求中按启用块存储的参数筛选访问权限	布尔型
eks:bootstrapClusterCreatorAdminPermissions	按创建集群请求中的 bootstrapClusterCreatorAdminPermissions 当前用户筛选访问权限	布尔型
eks:bootstrapSelfManagedAddons	按创建集群请求中存在的 bootstrapSelfManaged插件筛选访问权限	布尔型
eks:clientId	筛选用户向 EKS 服务发出的 C associateIdentityProviderConfig 请求中存在的 ClientId 的访问权限	字符串
eks:clusterName	按用户向 EKS 服务发出的访问条目请求中所包含的 clusterName 筛选访问权限	字符串

条件键	描述	类型
eks:computeConfigEnabled	在创建/更新集群请求中按启用计算配置的参数筛选访问权限	布尔型
eks:elasticLoadBalancingEnabled	在创建/更新集群请求中按启用弹性负载平衡的参数筛选访问权限	布尔型
eks:issuerUrl	按用户向 EKS 服务发出的 Confi associateIdentityProviderg 请求中存在的 issuerUrl 筛选访问权限	字符串
eks:kubernetesGroups	按用户向 EKS 服务发出的访问条目请求中所包含的 kubernetesGroups 筛选访问权限	ArrayOfString
eks:namespaces	按用户向 EKS 服务发出的关联/取消关联访问策略请求中包含的 namespaces 筛选访问权限	ArrayOfString
eks:policyArn	按用户向 EKS 服务发出的访问条目请求中所包含的 policyArn 筛选访问权限	ARN
eks:principalArn	按用户向 EKS 服务发出的访问条目请求中所包含的 principalArn 筛选访问权限	ARN
eks:supportType	按创建/更新集群请求中所包含的 supportType 筛选访问权限	字符串
eks:username	按用户向 EKS 服务发出的访问条目请求中所包含的 Kubernetes 用户名筛选访问权限	字符串

Amazon Elastic Load Balancing 的操作、资源和条件键

Amazon Elastic Load Balancing（服务前缀:`elasticloadbalancing`）提供以下特定于服务的资源、操作和条件上下文密钥，用于 IAM 权限策略。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。

- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Elastic Load Balancing 定义的操作
- Amazon Elastic Load Balancing 定义的资源类型
- Amazon Elastic Load Balancing 的条件键

Amazon Elastic Load Balancing 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddTags	授予将指定标签添加到指定负载均衡器的权限。每个负载均衡器最多可以有 10 个标签	标记	loadbalancer*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:CreateAction	
ApplySecurityGroupsToLoadBalancer	授予将一个或多个安全组关联到某个虚拟私有云（VPC）中的负载均衡器的权限	写入	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalanci	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				ng:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup	
AttachLoadBalancerToSubnets	授予向指定负载均衡器的已配置子网集中添加一个或多个子网的权限	写入	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:Subnet	
ConfigureHealthCheck	授予指定运行状况检查设置以在评估后端实例的运行状况时使用的权限	写入	loadbalancer*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateAppCookieStickinessPolicy	授予生成一个粘滞策略，并将其粘滞会话生命周期设置为遵循应用程序所生成 Cookie 的生命周期的权限	写入	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateLBCookieStickinessPolicy	授予生成一个粘滞策略，并将其粘滞会话生命周期设置由浏览器（用户代理）的生命周期控制，或者在指定期限后到期的权限	写入	loadbalancer*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateLoadBalancer	授予权限以创建负载均衡器	写入	loadbalancer		elasticloadbalancing:AddTags

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup elasticloadbalancing:Subnet elasticloadbalancing:Scheme elasticloadbalancing:Listen	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				erProtocol	
CreateLoadBalancerListeners	授予为指定负载均衡器创建一个或多个侦听器的权限	写入	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:ListenerProtocol	
CreateLoadBalancerPolicy	授予使用指定属性为指定负载均衡器创建一个策略的权限	写入	loadbalancer*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy	
DeleteLoadBalancer	授予删除指定负载均衡器的权限	写入	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteLoadBalancerListeners	授予从指定负载均衡器中删除指定侦听器的权限	写入	loadbalancer*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteLoadBalancerPolicy	授予从指定负载均衡器中删除指定策略的权限 不得为任何侦听器启用此策略	写入	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeregisterInstancesFromLoadBalancer	授予从指定负载均衡器中注销指定实例的权限	写入	loadbalancer*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DescribeInstanceHealth	授予描述指定实例中与指定负载均衡器有关的状态的权限	读取			
DescribeLoadBalancerAttributes	授予描述指定负载均衡器的属性的权限	读取			
DescribeLoadBalancerPolicies	授予描述指定策略的权限	读取			
DescribeLoadBalancerPolicyTypes	授予描述指定负载均衡器的策略类型的权限	读取			
DescribeLoadBalancers	授予描述指定的负载均衡器的权限。如果未指定负载均衡器，则该调用将描述您的所有负载均衡器	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeTags	授予描述与指定负载均衡器关联的标签的权限	读取			
DetachLoadBalancerFromSubnets	授予从负载均衡器的已配置子网集中移除指定子网的权限	写入	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DisableAvailabilityZonesForLoadBalancer	授予从指定负载均衡器的可用区集中移除指定可用区的权限	写入	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
EnableAvailabilityZonesForLoadBalancer	授予将指定可用区添加至指定负载均衡器的可用区集中的权限	写入	loadbalancer*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyLoadBalancerAttributes	授予修改指定负载均衡器的属性的权限	写入	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RegisterInstancesWithLoadBalancer	授予将指定实例添加到指定负载均衡器的权限	写入	loadbalancer*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveTags	授予从指定负载均衡器中移除一个或多个标签的权限	标记	loadbalancer*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
SetLoadBalancerListenerSSLCertificate	授予设置可终止指定侦听器的 SSL 连接的证书的权限	写入	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetLoadBalancerPoliciesForBackendServer	授予替换与指定端口关联的策略集，以便后端服务器用一组新策略在此端口上侦听的权限	写入	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetLoadBalancerPoliciesOfListener	授予将指定负载均衡器端口的当前策略集替换为指定策略集的权限	写入	loadbalancer*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy	

Amazon Elastic Load Balancing 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
loadbalancer	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/${LoadBalancerName}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

Amazon Elastic Load Balancing 的条件键

Amazon Elastic Load Balancing 定义了以下可用于 IAM 策略Condition元素的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中允许的标签键值对筛选访问	字符串
aws:ResourceTag/${TagKey}	按某个资源的标签键值对筛选访问	字符串
aws:TagKeys	按请求中允许的标签键列表筛选访问	ArrayOfString
elasticloadbalancing:CreateAction	按资源创建 API 操作的名称筛选访问	字符串
elasticloadbalancing:ListenerProtocol	按请求中允许的侦听器协议筛选访问权限	ArrayOfString
elasticloadbalancing:ResourceTag/	按附加到资源的标签键值对的前言字符串筛选访问	字符串
elasticloadbalancing:ResourceTag/${TagKey}	按附加到资源的标签键值对的前言字符串筛选访问	字符串
elasticloadbalancing:Scheme	按请求中允许的负载均衡器方案筛选访问权限	字符串

条件键	描述	类型
elasticloadbalancing:SecurityGroup	筛选请求中允许的安全组 IDs 的访问权限	ArrayOfString
elasticloadbalancing:SecurityPolicy	按请求中允许的 SSL 安全策略筛选访问权限	ArrayOfString
elasticloadbalancing:Subnet	按请求中允许 IDs 的子网筛选访问权限	ArrayOfString

Amazon Elastic Load Balancing V2 的操作、资源和条件键

Amazon Elastic Load Balancing V2（服务前缀:`elasticloadbalancing`）提供了以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Elastic Load Balancing V2 定义的操作
- Amazon Elastic Load Balancing V2 定义的资源类型
- Amazon Elastic Load Balancing V2 的条件键

Amazon Elastic Load Balancing V2 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddListenerCertificates	授予将指定证书添加至指定安全侦听器的权限	写入	listener/app*		
			listener/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				${TagKey}	
AddTags	授予将指定标签添加到指定负载均衡器的权限。每个负载均衡器最多可以有 10 个标签	标记	listener-rule/app		
			listener-rule/net		
			listener/app		
			listener/net		
			loadbalancer/app/		
			loadbalancer/net/		
			targetgroup		
			truststore		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:CreateAction	
AddTrustStoreRevocations	授予向信任存储添加撤销的权限	写入	truststore*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateListener	授予为指定应用程序负载均衡器创建侦听器的权限	写入	loadbalancer/app/		elasticloadbalancing:AddTags
			loadbalancer/net/		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy elasticloadbalancing:ListenerProtocol	
CreateLoadBalancer	授予权限以创建负载均衡器	写入	loadbalancer/app/		elasticloadbalancing:AddTags

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			loadbalancer/net/		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup elasticloadbalancing:Subnet elasticloadbalancing:Scheme	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateRule	授予为指定探测器创建规则的权限	写入	listener/app*		elasticloadbalancing:AddTags
			listener/net*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateTargetGroup	授予创建目标组的权限	写入	targetgroup*		elasticloadbalancing:AddTags

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateTrustStore	授予创建信任存储的权限	写入	truststore		elasticloadbalancing:AddTags

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteListener	授予删除指定侦听器的权限	写入	listener/app*		
			listener/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteLoadBalancer	授予删除指定负载均衡器的权限	写入	loadbalancer/app/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteRule	授予删除指定规则的权限	写入	listener-rule/app*		
			listener-rule/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteSharedTrustStoreAssociation	授予权限以删除指定共享信任存储关联	写入	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteTargetGroup	授予删除指定目标组的权限	写入	targetgroup*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteTrustStore	授予删除指定信任存储的权限	写入	truststore*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeregisterTargets	授予从指定目标组注销指定目标的权限	写入	targetgroup*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DescribeAccountLimits	授予描述 Elastic Load Balancing 资源限制的权限 Amazon Web Services 账户	读取			
DescribeCapacityReservation	授予描述负载均衡器容量预留的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeListenerAttributes	授予权限以描述指定侦听器的属性	读取			
DescribeListenerCertificates	授予描述指定安全侦听器的证书的权限	读取			
DescribeListeners	授予描述指定侦听器或指定应用程序负载均衡器的侦听器的权限	读取			
DescribeLoadBalancerAttributes	授予描述指定负载均衡器的属性的权限	读取			
DescribeLoadBalancers	授予描述指定的负载均衡器的权限。如果未指定负载均衡器，则该调用将描述您的所有负载均衡器	读取			
DescribeRules	授予描述指定规则或指定侦听器的规则的权限	读取			
DescribeSSLPolicies	授予描述指定策略或用于 SSL 协商的所有策略的权限	读取			
DescribeTags	授予描述与指定资源关联的标签的权限	读取			
DescribeTargetGroupAttributes	授予描述指定目标组的属性的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeTargetGroups	授予描述指定目标组或您的所有目标组的权限	读取			
DescribeTargetHealth	授予描述指定目标或您的所有目标的运行状况的权限	读取			
DescribeTrustStoreAssociations	授予描述信任存储的关联的权限	读取			
DescribeTrustStoreRevocations	授予描述指定信任存储撤销或与信任存储相关的所有撤销的权限	读取			
DescribeTrustStores	授予描述指定信任存储或您的所有信任存储的权限	读取			
GetResourcePolicy	授予权限以检索与资源关联的资源策略	读取	truststore		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
GetTrustStoreCaCertificatesBundle	授予检索信任存储 CA 证书捆绑包的权限	读取	truststore*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
GetTrustStoreRevocationContent	授予检索信任存储撤销内容的权限	读取	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyCapacityReservation	授予修改负载均衡器容量预留的权限	写入	loadbalancer/app/		
			loadbalancer/net/		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyIpPools	授予修改负载均衡器的 IP 池的权限	写入	loadbalancer/app/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyListener	授予修改指定侦听器的指定属性的权限	写入	listener/app*		
			listener/net*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy elasticloadbalancing:ListenerProtocol	
ModifyListenerAttributes	授予权限以修改指定侦听器的属性	写入	listener/app*		
			listener/net*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyLoadBalancerAttributes	授予修改指定负载均衡器的属性的权限	写入	loadbalancer/app/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyRule	授予修改指定规则的权限	写入	listener-rule/app*		
			listener-rule/net*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyTargetGroup	授予修改在评估指定目标组中目标的运行状况时所使用运行状况检查的权限	写入	targetgroup*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyTargetGroupAttributes	授予修改指定目标值的指定属性的权限	写入	targetgroup*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyTrustStore	授予修改指定信任存储的权限	写入	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RegisterTargets	授予将指定目标注册到指定目标组的权限	写入	targetgroup*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveListenerCertificates	授予移除指定安全侦听器的指定证书的权限	写入	listener/app*		
			listener/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveTags	授予从指定负载均衡器中移除一个或多个标签的权限	标记	listener-rule/app		
			listener-rule/net		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			listener/app		
			listener/net		
			loadbalancer/app/		
			loadbalancer/net/		
			targetgroup		
			truststore		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
RemoveTrustStoreRevocations	授予从信任存储中移除撤销的权限	写入	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetIpAddressType	授予设置指定负载均衡器的子网所使用 IP 地址类型的权限	写入	loadbalancer/app/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetRulePriorities	授予设置指定规则的优先级的权限	写入	listener-rule/app*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			listener-rule/net*		
SetSecurityGroups	授予将指定安全组关联到指定负载均衡器的权限	写入	loadbalancer/app/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup	
SetSubnets	授予为指定负载均衡器的指定子网启用可用区的权限	写入	loadbalancer/app/		
			loadbalancer/net/		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:Subnet	
SetWebAcl [仅权限]	授予向 WAF 授 WebAcl 予权限的权限	写入			

Amazon Elastic Load Balancing V2 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
listener/app	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener/app/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}`	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

资源类型	ARN	条件键
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}
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}

资源类型	ARN	条件键
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}

Amazon Elastic Load Balancing V2 的条件键

Amazon Elastic Load Balancing V2 定义了以下可用于 IAM 策略Condition元素的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中允许的标签键值对筛选访问	字符串
aws:ResourceTag/${TagKey}	按某个资源的标签键值对筛选访问	字符串
aws:TagKeys	按请求中允许的标签键列表筛选访问	ArrayOfString
elasticloadbalancing:CreateAction	按资源创建 API 操作的名称筛选访问	字符串

条件键	描述	类型
elasticloadbalancing:ListenerProtocol	按请求中允许的侦听器协议筛选访问权限	字符串
elasticloadbalancing:ResourceTag/${TagKey}	按附加到资源的标签键值对的前言字符串筛选访问	字符串
elasticloadbalancing:Scheme	按请求中允许的负载均衡器方案筛选访问权限	字符串
elasticloadbalancing:SecurityGroup	筛选请求中允许的安全组 IDs 的访问权限	ArrayOfString
elasticloadbalancing:SecurityPolicy	按请求中允许的 SSL 安全策略筛选访问权限	ArrayOfString
elasticloadbalancing:Subnet	按请求中允许 IDs 的子网筛选访问权限	ArrayOfString

Amazon Elastic 的操作、资源和条件密钥 MapReduce

Amazon Elastic MapReduce （服务前缀:`elasticmapreduce`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。

- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Elastic 定义的操作 MapReduce
- 由 Amazon Elastic 定义的资源类型 MapReduce
- 亚马逊 Elastic 的条件密钥 MapReduce

Amazon Elastic 定义的操作 MapReduce

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

> **Note**
>
> 该 DescribeJobFlows API 已被弃用，最终将被删除。我们建议您 ListBootstrapActions 改用 ListClusters DescribeCluster ListSteps、、 ListInstanceGroups 和

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddInstanceFleet	授予权限以将实例机群添加到运行的集群中	写入	cluster*		
AddInstanceGroups	授予权限以将实例组添加到运行的集群中	写入	cluster*		
AddJobFlowSteps	授予权限以将新步骤添加到运行的集群中	写入	cluster*		
				elasticmapreduce:ExecutionRoleArn	
AddTags	授予权限以将标签添加到 Amazon EMR 资源中	标记	cluster		
			editor		
			notebook-execution		
			studio		
				aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AttachEditor[仅权限]	授予权限以将 EMR 笔记本连接到计算引擎	写入	editor*		
CancelSteps	授予权限以取消运行的集群中的一个或多个待处理步骤	写入	cluster*		
CreateEditor[仅权限]	授予创建 EMR 笔记本的权限	写入	cluster		
				aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
CreatePersistentAppUI	授予创建永久性应用程序历史记录服务器的权限	写入	cluster*		
CreateRepository[仅权限]	授予创建 EMR 笔记本存储库的权限	写入			
CreateSecurityConfiguration	授予权限以创建安全配置	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateStudio	授予创建 EMR Studio 的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
CreateStudioPresignedUrl	授予使用 IAM 身份验证模式启动 EMR Studio 的权限	写入	studio*		
CreateStudioSessionMapping	授予创建 EMR Studio 会话映射的权限	写入	studio*		
DeleteEditor[仅权限]	授予删除 EMR 笔记本的权限	写入	editor*		
DeleteRepository[仅权限]	授予删除 EMR 笔记本存储库的权限	写入			
DeleteSecurityConfiguration	授予权限以删除安全配置	写入			
DeleteStudio	授予删除 EMR Studio 的权限	写入	studio*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteStudioSessionMapping	授予删除 EMR Studio 会话映射的权限	写入	studio*		
DeleteWorkspaceAccess[仅权限]	授予权限以阻止身份打开协作工作区	权限管理	editor*		
DescribeCluster	授予权限以获取有关集群的详细信息，包括状态、硬件和软件配置、VPC 设置等	读取	cluster*		
DescribeEditor[仅权限]	授予权限以查看有关笔记本的信息，包括状态、用户、角色、标签、位置等	读取	editor*		
DescribeJobFlows	授予描述集群详细信息（作业流）的权限。此 API 已弃用，最终将被删除。我们建议您 ListBootstrapActions 改用 ListClusters DescribeCluster ListSteps、、 ListInstanceGroups 和	读取	cluster*		
DescribeNotebookExecution	授予查看有关笔记本执行的信息的权限	读取	notebook-execution*		
DescribePersistentAppUI	授予描述永久性应用程序历史记录服务器的权限	读取	cluster*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeReleaseLabel	授予查看有关 EMR 版本的信息的权限，例如支持哪些应用程序	读取			
DescribeRepository[仅权限]	授予描述 EMR 笔记本存储库的权限	读取			
DescribeSecurityConfiguration	授予权限以获取安全配置的详细信息	读取			
DescribeStep	授予权限以获取有关集群步骤的详细信息	读取	cluster*		
DescribeStudio	授予查看有关 EMR Studio 的信息的权限	读取	studio*		
DetachEditor[仅权限]	授予从计算引擎分离 EMR 笔记本的权限	写入	editor*		
GetAutoTerminationPolicy	授予检索与集群关联的自动终止策略的权限	读取	cluster*		
GetBlockPublicAccessConfiguration	授予检索该地区的 EMR 屏蔽公共访问配置 Amazon Web Services 账户 的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetClusterSessionCredentials	授予为启用细粒度访问控制的 EMR 集群检索与给定执行 IAM 角色相关联的 HTTP 基本凭证的权限	写入	cluster*		
				elasticmapreduce:ExecutionRoleArn	
GetManagedScalingPolicy	授予检索与集群关联的托管扩缩策略的权限	读取	cluster*		
GetOnClusterAppUIPresignedURL	授予获取集群上运行的应用程序历史记录服务器的预签名 URL 的权限	写入	cluster*		
GetPersistentAppUIPresignedURL	授予获取永久应用程序历史记录服务器的预签名 URL 的权限	写入	cluster*		
				elasticmapreduce:ExecutionRoleArn	
GetStudioSessionMapping	授予查看有关 EMR Studio 会话映射的信息的权限	读取	studio*		
LinkRepository[仅权限]	授予将 EMR 笔记本存储库与 EMR Notebooks 链接的权限	写入			
ListBootstrapActions	授予权限以获取有关与集群关联的引导操作的详细信息	读取	cluster*		
ListClusters	授予获取可访问集群状态的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListEditors[仅权限]	授予列出可访问 EMR Notebooks 的摘要信息的权限	列表			
ListInstanceFleets	授予权限以获取集群中的实例机群的详细信息	读取	cluster*		
ListInstanceGroups	授予权限以获取集群中的实例组的详细信息	读取	cluster*		
ListInstances	授予获取有关集群中 Amazon EC2 实例详细信息的权限	读取	cluster*		
ListNotebookExecutions	授予列出笔记本执行摘要信息的权限	列表			
ListReleaseLabels	授予列出和筛选当前区域中可用 EMR 版本的权限	列表			
ListRepositories[仅权限]	授予列出现有 EMR 笔记本存储库的权限	列表			
ListSecurityConfigurations	授予权限以按名称列出该账户中的可用安全配置以及创建日期和时间	列表			
ListSteps	授予列出与集群关联的步骤的权限	读取	cluster*		
ListStudioSessionMappings	授予列出有关 EMR Studio 会话映射的摘要信息的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListStudios	授予列出有关 EMR Studios 摘要信息的权限	列表			
ListSupportedInstanceTypes	授予列出 Amazon EMR 版本支持的亚马逊 EC2 实例类型的权限	列表			
ListWorkspaceAccessIdentities[仅权限]	授予权限以列出被授予对工作区访问权限的身份	列表	editor*		
ModifyCluster	授予更改集群设置的权限，例如可为集群同时执行的步骤数	写入	cluster*		
ModifyInstanceFleet	授予权限以更改实例机群的目标按需容量和目标 Spot 容量	写入	cluster*		
ModifyInstanceGroups	授予更改实例组的 EC2 实例数量和配置的权限	写入	cluster		
OpenEditorInConsole[仅权限]	授予权限以从控制台中启动 EMR 笔记本的 Jupyter notebook 编辑器	写入	editor*		
			cluster		
PutAutoScalingPolicy	授予权限以便为核心实例组或任务实例组创建或更新弹性伸缩策略	写入	cluster*		
PutAutoTerminationPolicy	授予权限以创建或更新与集群关联的自动终止策略	写入	cluster*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutBlockPublicAccessConfiguration	授予权限以创建或更新该区域的 EMR 屏蔽公共访问配置 Amazon Web Services 账户	权限管理			
PutManagedScalingPolicy	授予权限以创建或更新与集群关联的托管扩缩策略	写入	cluster*		
PutWorkspaceAccess[仅权限]	授予权限以允许身份打开协作工作区	权限管理	editor*		
RemoveAutoScalingPolicy	授予从实例组中删除弹性伸缩策略的权限	写入	cluster*		
RemoveAutoTerminationPolicy	授予删除与集群关联的自动终止策略的权限	写入	cluster*		
RemoveManagedScalingPolicy	授予删除与集群关联的托管扩缩策略的权限	写入	cluster*		
RemoveTags	授予从 Amazon EMR 资源中删除标签的权限	标记	cluster		
			editor		
			notebook-execution		
			studio		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys	
RunJobFlow	授予创建和启动集群（任务流）的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	iam:PassRole
SetKeepJobFlowAliveWhenNoSteps	授予权限以在集群执行步骤后添加和移除自动终止	写入	cluster*		
SetTerminationProtection	授予权限以便为集群添加和删除终止保护	写入	cluster*		
SetUnhealthyNodeReplacement	授予权限以为集群启用或禁用运行状况不佳的节点替换	写入	cluster*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
SetVisibleToAllUsers	授予权限以设置是否所有 Amazon 身份和访问管理 (IAM) Access Management 用户都可以查看集群。 Amazon Web Services 账户 此 API 已被弃用，您的集群可能对账户中的所有用户都可见。要使用 IAM 策略限制集群访问权限，请参阅 Amazon EMR 的 Ident Amazon ity and Access 管理 (https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-plan-access-iam .html)	写入	cluster*		
StartEditor[仅权限]	授予启动 EMR 笔记本的权限	写入	editor*		
			cluster		
StartNotebookExecution	授予启动 EMR 笔记本执行的权限	写入	cluster*		
			editor*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
StopEditor[仅权限]	授予关闭 EMR 笔记本的权限	写入	editor*		
StopNotebookExecution	授予停止笔记本执行的权限	写入	notebook-execution*		
TerminateJobFlows	授予终止集群（任务流）的权限	写入	cluster*		
UnlinkRepository[仅权限]	授予取消 EMR 笔记本存储库与 EMR Notebooks 链接的权限	写入			
UpdateEditor[仅权限]	授予权限以更新 EMR Notebooks	写入	editor*		
UpdateRepository[仅权限]	授予更新 EMR 笔记本存储库的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateStudio	授予更新有关 EMR Studio 的信息的权限	写入	studio*		
UpdateStudioSessionMapping	授予更新 EMR Studio 会话映射的权限	写入	studio*		
ViewEventsFromAllClustersInConsole[仅权限]	授予权限以使用 EMR 控制台查看所有集群中的事件	列表			

由 Amazon Elastic 定义的资源类型 MapReduce

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}

资源类型	ARN	条件键
		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}

亚马逊 Elastic 的条件密钥 MapReduce

Amazon Elastic MapReduce 定义了以下条件密钥，这些条件键可用于 IAM 策略的Condition元素中。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按是否随操作一起提供标签和值对筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与 Amazon EMR 资源关联的标签和值对筛选访问权限	字符串
aws:TagKeys	按是否随操作一起提供标签键筛选访问权限，而不管标签值如何	ArrayOfString

条件键	描述	类型
elasticmapreduce:ExecutionRoleArn	按是否随操作一起提供执行角色 ARN 筛选访问权限	ARN
elasticmapreduce:RequestTag/${TagKey}	按是否随操作一起提供标签和值对筛选访问权限	字符串
elasticmapreduce:ResourceTag/${TagKey}	按与 Amazon EMR 资源关联的标签和值对筛选访问权限	字符串

Amazon 的操作、资源和条件密钥 ElastiCache

Amazon ElastiCache （服务前缀:`elasticache`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon 定义的操作 ElastiCache
- Amazon 定义的资源类型 ElastiCache
- Amazon 的条件密钥 ElastiCache

Amazon 定义的操作 ElastiCache

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

> **Note**
>
> 在 IAM 中创建 ElastiCache 策略时，必须为资源块使用 “*” 通配符。有关在 IAM 策略中使用以下 ElastiCache API 操作的信息，请参阅 A mazon ElastiCache 用户指南中的ElastiCache 操作和 IAM。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddTagsToResource	授予向 ElastiCache 资源添加标签的权限	标记	cluster		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			parameter group		
			replicationgroup		
			reserved-instance		
			securitygroup		
			serverlesscache		
			serverlesscachesnapshot		
			snapshot		
			subnetgroup		
			user		
			usergroup		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
AuthorizeCacheSecurityGroupIngress	授予在 EC2 安全组上授权 ElastiCache 安全组的权限	写入	securitygroup*		ec2:AuthorizeSecurityGroupIngress
				aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchApplyUpdateAction	授予将 ElastiCache 服务更新应用于群集和复制组组的权限	写入	cluster		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs s3:GetObject
			replicationgroup		
				aws:ResourceTag/${TagKey}	
BatchStopUpdateAction	授予阻止在一组集群上执行 ElastiCache 服务更新的权限	写入	cluster		
			replicationgroup		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey}	
CompleteMigration	授予完成将数据从亚马逊 EC2 上托管的 Redis 在线迁移到 ElastiCache	写入	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
Connect	授予以指定 ElastiCache 用户身份连接到 ElastiCache 复制组或 ElastiCache 无服务器缓存的权限	写入	user*		
			replicationgroup		
			serverlesscache		
				aws:ResourceTag/${TagKey}	
CopyServerlessCacheSnapshot	授予复制现有无服务器缓存快照的权限	写入	serverlesscachesnapshot*	aws:ResourceTag/${TagKey} elasticache:KmsKeyId	elasticache:AddTagsToResource

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
CopySnapshot	授予权限以复制现有快照	Write	snapshot*		elasticache:AddTagsToResource s3:DeleteObject s3:GetBucketAcl s3:PutObject
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys elasticache:KmsKeyId	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateCacheCluster	授予权限以创建缓存集群	Write	parametergroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs elasticache:AddTagsToResource s3:GetObject

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			cluster	aws:RequestTag/${TagKey} aws:TagKeys elasticache:CacheNodeType elasticache:EngineVersion elasticache:EngineType elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:CacheP	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				arameterGroupName	
			replicationgroup	elasticache:CacheNodeType elasticache:EngineVersion elasticache:EngineType elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:CacheParameterGroupName	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			securitygroup		
			snapshot		
			subnetgroup		
				aws:ResourceTag/${TagKey}	
CreateCacheParameterGroup	授予权限以创建参数组	Write	parametergroup*		elasticache:AddTagsToResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys elasticache:CacheParameterGroupName	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateCacheSecurityGroup	授予权限以创建缓存安全组	Write	securitygroup*		elasticache:AddTagsToResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateCacheSubnetGroup	授予权限以创建缓存子网组	Write	subnetgroup*		elasticache:AddTagsToResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateGlobalReplicationGroup	授予权限以创建全局复制组	Write	globalreplicationgroup*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			replicationgroup*		
				aws:ResourceTag/${TagKey}	
CreateReplicationGroup	授予权限以创建复制组	写入	parametergroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs elasticache:AddTagsToResource s3:GetObject

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			cluster		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			globalreplicationgroup	elasticache:NumNodeGroups elasticache:CacheNodeType elasticache:ReplicasPerNodeGroup elasticache:EngineVersion elasticache:EngineType elasticache:AtRestEncryptionEnabled elasticache:TransitEncryptionEnabled elasticache:AutomaticFailoverEnabled	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				elasticache:MultiAZEnabled elasticache:ClusterModeEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:KmsKeyId elasticache:CacheParameterGroupName	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			replicationgroup	aws:RequestTag/${TagKey} aws:TagKeys elasticache:NumNodeGroups elasticache:CacheNodeType elasticache:ReplicasPerNodeGroup elasticache:EngineVersion elasticache:EngineType elasticache:AtRestEncryptionEnabled elasticache:Transi	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				tEncryptionEnabled elasticache:AutomaticFailoverEnabled elasticache:MultiAZEnabled elasticache:ClusterModeEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:KmsKeyId elasticache:CacheParameterGroupName	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			securitygroup		
			snapshot		
			subnetgroup		
			usergroup		
				aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateServerlessCache	授予创建无服务器缓存的权限	写入	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

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				elasticache:MinimumECPUPerSecond elasticache:MaximumECPUPerSecond	s3:GetObject
			serverlessscachesnapshot	aws:ResourceTag/${TagKey}	
			snapshot	aws:ResourceTag/${TagKey}	
			usergroup	aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateServerlessCacheSnapshot	授予在特定时刻创建无服务器缓存副本的权限	写入	serverlesscache*	aws:ResourceTag/${TagKey}	elasticache:AddTagsToResource

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			serverlessscachesnapshot*	aws:ResourceTag/${TagKey} elasticache:KmsKeyId	
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshot	授予权限以在特定时刻及时创建整个 Redis 集群的副本	写入	snapshot*	aws:RequestTag/${TagKey} aws:TagKeys elasticache:KmsKeyId	elasticache:AddTagsToResource s3:DeleteObject s3:GetBucketAcl s3:PutObject
			cluster		
			replicationgroup		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey}	
CreateUser	授予权限以创建 Redis 的用户。Redis 6.0 及更高版本支持用户	写入	user*		elasticache:AddTagsToResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys elasticache:UserAuthenticationMode	
CreateUserGroup	授予权限以创建 Redis 的用户组。Redis 6.0 及更高版本支持组	写入	user*		elasticache:AddTagsToResource

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			usergroup*	aws:RequestTag/${TagKey} aws:TagKeys	
				aws:ResourceTag/${TagKey}	
DecreaseNodeGroupsInGlobalReplicationGroup	授予权限以减少全局复制组中节点组的数量	Write	globalreplicationgroup*		
				elasticache:NumNodeGroups	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DecreaseReplicaCount	授予权限以减少 Redis（已禁用集群模式）复制组中的副本数量或 Redis（已启用集群模式）复制组中一个或多个节点组（分区）中的副本节点数量	Write	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey} elasticache:ReplicasPerNodeGroup	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteCacheCluster	授予权限以删除以前预配置的集群	Write	cluster*	aws:ResourceTag/${TagKey}	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			snapshot		
DeleteCacheParameterGroup	授予权限以删除指定缓存参数组	Write	parametergroup*		
				aws:ResourceTag/${TagKey} elasticache:CacheParameterGroupName	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteCacheSecurityGroup	授予权限以删除缓存安全组	Write	securitygroup*		
				aws:ResourceTag/${TagKey}	
DeleteCacheSubnetGroup	授予权限以删除缓存子网组	Write	subnetgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	
DeleteGlobalReplicationGroup	授予权限以删除现有全局复制组	Write	globalreplicationgroup*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteReplicationGroup	授予权限以删除现有复制组	写入	replicationgroup*	aws:ResourceTag/${TagKey}	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			snapshot		
DeleteServerlessCache	授予删除无服务器缓存的权限	写入	serverlesscache*	aws:ResourceTag/${TagKey}	ec2:DescribeTags
			serverlesscachesnapshot		
DeleteServerlessCacheSnapshot	授予删除无服务器缓存快照的权限	写入	serverlesscachesnapshot*	aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteSnapshot	授予权限以删除现有快照	Write	snapshot*		
				aws:ResourceTag/${TagKey}	
DeleteUser	授予权限以删除现有用户，从而将其从分配给它的所有用户组和复制组中删除	Write	user*		
				aws:ResourceTag/${TagKey}	
DeleteUserGroup	授予权限以删除现有用户组	Write	usergroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheClusters	授予权限以列出有关预置缓存集群的信息	列表	cluster*		
				aws:ResourceTag/${TagKey}	
DescribeCacheEngineVersions	授予列出可用缓存引擎及其版本的权限	列表			
DescribeCacheParameterGroups	授予权限以列出缓存参数组描述	List	parametergroup*		
				aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeCacheParameters	授予权限以检索特定缓存参数组的详细参数列表	List	parametergroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheSecurityGroups	授予权限以列出缓存安全组描述	List	securitygroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheSubnetGroups	授予权限以列出缓存子网组描述	List	subnetgroup*		
				aws:ResourceTag/${TagKey}	
DescribeEngineDefaultParameters	授予权限以检索指定缓存引擎的默认引擎和系统参数信息	List			
DescribeEvents	授予权限以列出与集群、缓存安全组和缓存参数组相关的事件	List			
DescribeGlobalReplicationGroups	授予权限以列出有关全局复制组的信息	List	globalreplicationgroup*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeReplicationGroups	授予权限以列出有关预置复制组的信息	List	replicationgroup*		
				aws:ResourceTag/${TagKey}	
DescribeReservedCacheNodes	授予权限以列出有关购买的预留缓存节点的信息	List	reserved-instance*		
				aws:ResourceTag/${TagKey}	
DescribeReservedCacheNodesOfferings	授予权限以获取可用的预留缓存节点产品	列表			
DescribeServerlessCacheSnapshots	授予列出无服务器缓存快照信息的权限	列表	serverlesscachesnapshot*	aws:ResourceTag/${TagKey}	
			serverlesscache	aws:ResourceTag/${TagKey}	
DescribeServerlessCaches	授予列出无服务器缓存的权限	列表	serverlesscache*	aws:ResourceTag/${TagKey}	
DescribeServiceUpdates	授予权限以列出服务更新详细信息	List			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeSnapshots	授予权限以列出有关集群或复制组快照的信息	List	snapshot*		
				aws:ResourceTag/${TagKey}	
DescribeUpdateActions	授予权限以列出一组集群或复制组的更新操作详细信息	List	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
DescribeUserGroups	授予权限以列出有关 Redis 用户组的信息	List	usergroup*		
				aws:ResourceTag/${TagKey}	
DescribeUsers	授予权限以列出有关 Redis 用户的信息	List	user*		
				aws:ResourceTag/${TagKey}	
DisassociateGlobalReplicationGroup	授予权限以从全局复制组中删除辅助复制组	写入	globalreplicationgroup*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ExportServerlessCacheSnapshot	授予在指定时刻将无服务器缓存副本导出到 S3 存储桶的权限	写入	serverlesscachesnapshot*	aws:ResourceTag/${TagKey}	s3:DeleteObject s3:ListAllMyBuckets s3:PutObject
FailoverGlobalReplicationGroup	授予权限以将主区域故障转移到全局复制组的选定辅助区域	Write	globalreplicationgroup*		
IncreaseNodeGroupsInGlobalReplicationGroup	授予权限以增加全局复制组中节点组的数量	Write	globalreplicationgroup*		
				elasticache:NumNodeGroups	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
IncreaseReplicaCount	授予权限以增加 Redis（已禁用集群模式）复制组中的副本数量或 Redis（已启用集群模式）复制组中一个或多个节点组（分区）中的副本节点数量	写入	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey} elasticache:ReplicasPerNodeGroup	
InterruptClusterAzPower[仅权限]	授予测试 ElastiCache 资源可用区电源中断的权限	写入	replicationgroup*		
				aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListAllowedNodeTypeModifications	授予权限以列出可用于扩展特定 Redis 集群或复制组的可用节点类型	列表	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
ListTagsForResource	授予列出 ElastiCache 资源标签的权限	读取	cluster		
			parametergroup		
			replicationgroup		
			reserved-instance		
			securitygroup		
			serverlesscache		
			serverlesscachesnapshot		
			snapshot		
			subnetgroup		
			user		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			usergroup		
				aws:ResourceTag/${TagKey}	
ModifyCacheCluster	授予权限以修改集群的设置	Write	cluster*	elasticache:CacheNodeType elasticache:EngineVersion elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:CacheParameterGroupName	
			parametergroup		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			securitygroup		
				aws:ResourceTag/${TagKey}	
ModifyCacheParameterGroup	授予权限以修改缓存参数组的参数	Write	parametergroup*		
				aws:ResourceTag/${TagKey} elasticache:CacheParameterGroupName	
ModifyCacheSubnetGroup	授予权限以修改现有缓存子网组	Write	subnetgroup*		
				aws:ResourceTag/${TagKey}	
ModifyGlobalReplicationGroup	授予权限以修改全局复制组的设置	Write	globalreplicationgroup*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				elasticache:CacheNodeType elasticache:EngineVersion elasticache:AutomaticFailoverEnabled	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ModifyReplicationGroup	授予权限以修改复制组的设置	Write	replicationgroup*	elasticache:CacheNodeType elasticache:EngineVersion elasticache:AutomaticFailoverEnabled elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:CacheParameterGroupName elasticache:TransitEncrypti	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				onEnabled elasticache:ClusterModeEnabled	
			parametergroup		
			securitygroup		
			usergroup		
				aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ModifyReplicationGroupShardConfiguration	授予权限以在复制组现有分区之间添加分区、删除分区或重新平衡密钥空间	写入	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey} elasticache:NumNodeGroups	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ModifyServerlessCache	授予修改无服务器缓存参数的权限	写入	serverlesscache*	aws:ResourceTag/${TagKey} elasticache:EngineVersion elasticache:SnapshotRetentionLimit elasticache:MinimumDataStorage elasticache:MaximumDataStorage elasticache:DataStorageUnit elasticache:MinimumECPUPerSecond elasticache:Maximu	ec2:DescribeSecurityGroups ec2:DescribeTags

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				mECPUPerSecond	
			usergroup	aws:ResourceTag/${TagKey}	
ModifyUser	授予权限以更改 Redis 用户密码和/或访问字符串	Write	user*		
				aws:ResourceTag/${TagKey} elasticache:UserAuthenticationMode	
ModifyUserGroup	授予权限以更改属于用户组的用户列表	Write	user*		
			usergroup*		
				aws:ResourceTag/${TagKey}	
PurchaseReservedCacheNodesOffering	授予权限以购买预留缓存节点产品	Write	reserved-instance*		elasticache:AddTagsToResource

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
RebalanceSlotsInGlobalReplicationGroup	授予权限以执行密钥空间重新平衡操作，以重新分发插槽并确保在全局复制组中的现有分区之间进行密钥的统一分配	Write	globalreplicationgroup*		
RebootCacheCluster	授予权限以重新启动预置缓存集群或复制组中的部分或全部缓存节点（已禁用集群模式）	写入	cluster*		
				aws:ResourceTag/${TagKey}	
RemoveTagsFromResource	授予从 ElastiCache 资源中移除标签的权限	标记	cluster		
			parametergroup		
			replicationgroup		
			reserved-instance		
			securitygroup		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			serverlesscache		
			serverlesscachesnapshot		
			snapshot		
			subnetgroup		
			user		
			usergroup		
				aws:TagKeys aws:ResourceTag/${TagKey}	
ResetCacheParameterGroup	授予权限以将缓存参数组的参数改回其默认值	写入	parametergroup*		
				aws:ResourceTag/${TagKey} elasticache:CacheParameterGroupName	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
RevokeCacheSecurityGroupIngress	授予从安全组中移除 EC2 安全组入口的 ElastiCache 权限	写入	securitygroup*		
				aws:ResourceTag/${TagKey}	
StartMigration	授予开始将数据从亚马逊上托管的 Redis 迁移 EC2 到 Redis ElastiCache 的权限	写入	replicationgroup*		
				aws:ResourceTag/${TagKey}	
TestFailover	授予权限以测试复制组中的指定节点组上的自动故障转移	写入	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey}	
TestMigration	授予测试从亚马逊托管的 Redis 到 Redis 的数据迁 EC2 移 ElastiCache 的权限	写入	replicationgroup*		
				aws:ResourceTag/${TagKey}	

Amazon 定义的资源类型 ElastiCache

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}

资源类型	ARN	条件键
		aws:ResourceTag/${TagKey} aws:TagKeys
subnetgroup	arn:${Partition}:elasticache:${Region}:${Account}:subnetgroup:${CacheSubnetGroupName}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

资源类型	ARN	条件键
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 elasticache:NumNodeGroups

资源类型	ARN	条件键
		elasticache:ReplicasPerNodeGroup elasticache:SnapshotRetentionLimit elasticache:TransitEncryptionEnabled
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

资源类型	ARN	条件键
reserved-instance	arn:${Partition}:elasticache:${Region}:${Account}:reserved-instance:${ReservedCacheNodeId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
snapshot	arn:${Partition}:elasticache:${Region}:${Account}:snapshot:${SnapshotName}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:KmsKeyId

资源类型	ARN	条件键
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

资源类型	ARN	条件键
		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

资源类型	ARN	条件键
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

资源类型	ARN	条件键
serverlesscachesnapshot	arn:${Partition}:elasticache:${Region}:${Account}:serverlesscachesnapshot:${ServerlessCacheSnapshotName}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:KmsKeyId

Amazon 的条件密钥 ElastiCache

Amazon ElastiCache 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

> **Note**
>
> 要使用字符串类型的条件键构造条件元素，请使用不区分大小写的条件运算符 StringEqualsIgnoreCase 或 StringNotEqualsIgnoreCase 将键与字符串值进行比较。
> 有关 IAM 策略中控制访问权限的条件的信息 ElastiCache，请参阅 A mazon ElastiCache 用户指南中的ElastiCache 密钥。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中传递的标签筛选操作	字符串
aws:ResourceTag/${TagKey}	根据与资源关联的标签筛选操作	字符串
aws:TagKeys	根据在请求中传递的标签键筛选操作	ArrayOfString

条件键	描述	类型
elasticache:AtRestEncryptionEnabled	按请求中存在的 AtRestEncryptionEnabled 参数过滤访问权限，如果参数不存在，则按默认 false 值过滤访问权限	布尔型
elasticache:AuthTokenEnabled	通过请求中是否存在非空 AuthToken 参数来筛选访问权限	布尔型
elasticache:AutomaticFailoverEnabled	按请求中的 AutomaticFailoverEnabled 参数筛选访问权限	布尔型
elasticache:CacheNodeType	按请求中存在的 cacheNodeType 参数筛选访问权限。此密钥可用于限制在集群创建或扩展操作中使用哪些缓存节点类型	字符串
elasticache:CacheParameterGroupName	按请求中的 CacheParameterGroupName 参数筛选访问权限	字符串
elasticache:ClusterModeEnabled	按请求中存在的集群模式参数筛选访问。单节点组（分区）创建的默认值为 false	布尔型
elasticache:DataStorageUnit	按以下方式筛选访问权限 CacheUsageLimits。 DataStorage.Unit 参数在 CreateServerlessCache 和 ModifyServerlessCache 请求中	字符串
elasticache:EngineType	按创建请求中存在的引擎类型筛选访问。对于创建复制组，如果参数不存在，则使用默认引擎“redis”作为键	字符串
elasticache:EngineVersion	按创建或集群修改请求中存在的 engineVersion 参数筛选访问	字符串

条件键	描述	类型
elasticache:KmsKeyId	按 KMS 密钥的密钥 ID 筛选访问权限	字符串
elasticache:MaximumDataStorage	按以下方式筛选访问权限 CacheUsageLimits。 DataStorage.and 请求中的 CreateServerlessCache 最大参数 ModifyServerlessCache	数值
elasticache:MaximumECPUPerSecond	按以下方式筛选访问权限 CacheUsageLimits。 ECPUPerSecond.Maximum 参数在和请求中 CreateServerlessCache ModifyServerlessCache	数值
elasticache:MinimumDataStorage	按以下方式筛选访问权限 CacheUsageLimits。 DataStorage.and 请求中的最 CreateServerlessCache 小 ModifyServerlessCache 参数	数值
elasticache:MinimumECPUPerSecond	按以下方式筛选访问权限 CacheUsageLimits。 ECPUPerSecond.minimum 参数在和请求中 CreateServerlessCache ModifyServerlessCache	数值
elasticache:MultiAZEnabled	按 AZMode 参数、多AZEnabled 参数或集群或复制组可以放置的可用区数量筛选访问权限	布尔型
elasticache:NumNodeGroups	按请求中指定的 NumNodeGroups 或 NodeGroupCount 参数筛选访问权限。此密钥可用于限制创建或扩展操作后集群可以拥有的节点组（分区）的数量	数值
elasticache:ReplicasPerNodeGroup	按创建或扩展请求中指定的每个节点组（分区）的副本数筛选访问	数值
elasticache:SnapshotRetentionLimit	按请求中的 SnapshotRetentionLimit 参数筛选访问权限	数值

条件键	描述	类型
elasticache:TransitEncryptionEnabled	按请求中存在的 TransitEncryptionEnabled 参数筛选访问权限。在创建复制组时，如果参数不存在，则使用默认值“false”作为键	布尔型
elasticache:UserAuthenticationMode	按请求中的 UserAuthenticationMode 参数筛选访问权限	字符串

Amazon 元素的动作、资源和条件键 MediaConvert

Amazon Elemental MediaConvert （服务前缀:`mediaconvert`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- 由 Amazon Elemental 定义的动作 MediaConvert
- 由 Amazon Elemental 定义的资源类型 MediaConvert
- Amazon 元素的条件键 MediaConvert

由 Amazon Elemental 定义的动作 MediaConvert

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须

具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateCertificate	授予将 Amazon 证书管理器 (ACM) 亚马逊资源名称 (ARN) 与 Elemental 关联的权限 Amazon MediaConvert	写入			
CancelJob	授予取消队列中正在等待的 Amazon 元素 MediaConvert 任务的权限	写入	Job*		
CreateJob	授予创建和提交 Amazon 元素 MediaConvert 任务的权限	写入	JobTemplate		
			Preset		
			Queue		
				aws:RequestTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys mediaconvert:HttpInputsAllowed mediaconvert:HttpsInputsAllowed mediaconvert:S3InputsAllowed	
CreateJobTemplate	授予创建 Amazon Elemental MediaConvert 自定义作业模板的权限	写入	Preset		
			Queue		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePreset	授予创建 Amazon Elemental MediaConvert 自定义输出预设的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateQueue	授予创建 Amazon 元素 MediaConvert 任务队列的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteJobTemplate	授予删除 Amazon Elemental MediaConvert 自定义作业模板的权限	写入	JobTemplate*		
DeletePolicy	授予删除 Amazon 元素 MediaConvert 策略的权限	写入			
DeletePreset	授予删除 Amazon Elemental MediaConvert 自定义输出预设的权限	写入	Preset*		
DeleteQueue	授予删除 Amazon 元素 MediaConvert 任务队列的权限	写入	Queue*		
DescribeEndpoints	通过发送账户特定端点的请求，授予订阅 Amazon Elemental MediaConvert 服务的权限。必须将所有转码请求发送到服务返回的端点	列表			
DisassociateCertificate	授予移除 Certifice Manager (ACM) Amazon 证书的亚马逊资源名称 (ARN) 与 Elemental 资源之间关联的权限 Amazon MediaConvert	写入			
GetJob	授予获得 Amazon 元素 MediaConvert 任务的权限	读取	Job*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetJobTemplate	授予获取 Amazon 元素 MediaConvert 作业模板的权限	读取	JobTemplate*		
GetPolicy	授予获取 Amazon 元素 MediaConvert 策略的权限	读取			
GetPreset	授予获取 Amazon 元素 MediaConvert 输出预设的权限	读取	Preset*		
GetQueue	授予获取 Amazon 元素 MediaConvert 任务队列的权限	读取	Queue*		
ListJobTemplates	授予列出 Amazon Elemental MediaConvert 作业模板的权限	列表			
ListJobs	授予列出 Amazon 元素 MediaConvert 任务的权限	列表	Queue		
ListPresets	授予列出 Amazon 元素 MediaConvert 输出预设的权限	列表			
ListQueues	授予列出 Amazon Elemental MediaConvert 任务队列的权限	列表			
ListTagsForResource	授予检索队 MediaConvert 列、预设或作业模板标签的权限	读取	JobTemplate		
			Preset		
			Queue		
ListVersions	授予列出 Amazon Elemental MediaConvert 作业引擎版本的权限	列表			
Probe	授予探查文件的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutPolicy	授予放置 Amazon 元素 MediaConvert 策略的权限	写入			
SearchJobs	授予搜索 Amazon 元素 MediaConvert 任务的权限	列表	Queue		
TagResource	授予向 MediaConvert 队列、预设或作业模板添加标签的权限	标记	JobTemplate		
			Preset		
			Queue		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予从 MediaConvert 队列、预设或作业模板中移除标签的权限	标记	JobTemplate		
			Preset		
			Queue		
				aws:TagKeys	
UpdateJobTemplate	授予更新 Amazon Elemental MediaConvert 自定义作业模板的权限	写入	JobTemplate*		
			Preset		
			Queue		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdatePreset	授予更新 Amazon Elemental MediaConvert 自定义输出预设的权限	写入	Preset*		
UpdateQueue	授予更新 Amazon 元素 MediaConvert 任务队列的权限	写入	Queue*		

由 Amazon Elemental 定义的资源类型 MediaConvert

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
Job	arn:${Partition}:mediaconvert:${Region}:${Account}:jobs/${JobId}	aws:ResourceTag/${TagKey}
Queue	arn:${Partition}:mediaconvert:${Region}:${Account}:queues/${QueueName}	aws:ResourceTag/${TagKey}
Preset	arn:${Partition}:mediaconvert:${Region}:${Account}:presets/${PresetName}	aws:ResourceTag/${TagKey}
JobTemplate	arn:${Partition}:mediaconvert:${Region}:${Account}:jobTemplates/${JobTemplateName}	aws:ResourceTag/${TagKey}
CertificateAssociation	arn:${Partition}:mediaconvert:${Region}:${Account}:certificates/${CertificateArn}	

Amazon 元素的条件键 MediaConvert

Amazon Elemental MediaConvert 定义了以下可以在 IAM 策略Condition元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中的标签键值对筛选访问	字符串
aws:ResourceTag/${TagKey}	按附加到资源的标签键值对筛选操作	字符串
aws:TagKeys	按请求中的标签键筛选访问权限	ArrayOfString
mediaconvert:HttpInputsAllowed	通过账户中存在的 HTTP 输入策略筛选访问权限	布尔型
mediaconvert:HttpsInputsAllowed	通过账户中存在的 HTTPS 输入策略筛选访问权限	布尔型
mediaconvert:S3InputsAllowed	通过账户中存在的 S3 输入策略筛选访问权限	布尔型

Amazon EMR Serverless 的操作、资源和条件键

Amazon EMR Serverless（服务前缀：emr-serverless）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。

- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon EMR Serverless 定义的操作
- Amazon EMR Serverless 定义的资源类型
- Amazon EMR Serverless 的条件键

Amazon EMR Serverless 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AccessInteractiveEndpoints[仅权限]	授予在应用程序上执行交互式工作负载的权限	写入	application*		iam:PassRole
AccessLivyEndpoints[仅权限]	授予权限以在 EMR Serverless Application 启用的 Livy 端点上执行交互式工作负载	写入	application*		iam:PassRole
CancelJobRun	授予取消作业运行的权限	写入	jobRun*		
CreateApplication	授予创建应用程序的权限	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	授予删除应用程序的权限	写入	application*		
GetApplication	授予获取应用程序的权限	读取	application*		
GetDashboardForJobRun	授予获取任务运行控制面板的权限	读取	jobRun*		
GetJobRun	授予获取任务运行的权限	读取	jobRun*		
ListApplications	授予列出应用程序的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListJobRunAttempts	授予权限以列出与作业运行关联的作业运行尝试	列表	jobRun*		
ListJobRuns	授予列出与应用程序关联的任务运行的权限	列表	application*		
ListTagsForResource	授予列出指定资源的标签的权限	读取	application		
			jobRun		
StartApplication	授予启动应用程序的权限	写入	application*		
StartJobRun	授予启动作业运行的权限	写入	application*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
StopApplication	授予停止应用程序的权限	写入	application*		
TagResource	授予标记指定资源的权限	Tagging	application		
			jobRun		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予取消标记指定资源的权限	标记	application		
			jobRun		
				aws:TagKeys	
UpdateApplication	授予更新应用程序的权限	写入	application*		

Amazon EMR Serverless 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}

Amazon EMR Serverless 的条件键

Amazon EMR Serverless 定义以下可以在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对来筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按附加到资源的标签键值对筛选操作	字符串
aws:TagKeys	根据在请求中是否具有标签键来筛选访问	ArrayOfString

Amazon 的操作、资源和条件密钥 EventBridge

Amazon EventBridge （服务前缀:events）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon 定义的操作 EventBridge
- Amazon 定义的资源类型 EventBridge
- Amazon 的条件密钥 EventBridge

Amazon 定义的操作 EventBridge

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ActivateEventSource	授予激活合作伙伴事件源的权限	Write	event-source*		
CancelReplay	授予取消重播的权限	Write	replay*		
CreateApiDestination	授予创建新 api 目标的权限	Write	api-destination*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			connection*		
CreateArchive	授予创建新存档的权限	Write	archive*		
			event-bus*		
CreateConnection	授予创建新连接的权限	写入	connection*		
CreateEndpoint	授予权限以创建终端节点	写入	endpoint*		
				events:EventBusArn	
CreateEventBus	授予创建事件总线的权限	Write	event-bus*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePartnerEventSource	授予创建合作伙伴事件源的权限	Write	event-source*		
DeactivateEventSource	授予停用事件源的权限	Write	event-source*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeauthorizeConnection	授予取消连接授权的权限，删除其存储的授权密钥	Write	connection*		
DeleteApiDestination	授予删除 api 目标的权限	Write	api-destination*		
DeleteArchive	授予删除存档的权限	Write	archive*		
DeleteConnection	授予权限以删除连接	写入	connection*		
DeleteEndpoint	授予权限以删除终端节点	写入	endpoint*		
DeleteEventBus	授予删除事件总线的权限	Write	event-bus*		
DeletePartnerEventSource	授予删除合作伙伴事件源的权限	Write	event-source*		
DeleteRule	授予删除规则的权限	Write	rule-on-custom-event-bus		
			rule-on-default-event-bus		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				events:creatorAccount events:ManagedBy	
DescribeApiDestination	授予检索 api 目标详细信息的权限	Read	api-destination*		
			connection*		
DescribeArchive	授予检索存档详细信息的权限	Read	archive*		
DescribeConnection	授予检索连接详细信息的权限	读取	connection*		
DescribeEndpoint	授予权限以检索有关终端节点的详细信息	读取	endpoint*		
DescribeEventBus	授予检索事件总线详细信息的权限	Read	event-bus		
DescribeEventSource	授予检索事件源详细信息的权限	Read	event-source*		
DescribePartnerEventSource	授予检索合作伙伴事件源详细信息的权限	Read	event-source*		
DescribeReplay	授予检索重播详细信息的权限	Read	replay*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeRule	授予检索规则详细信息的权限	Read	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount	
DisableRule	授予禁用规则的权限	写入	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount events:ManagedBy	
EnableRule	授予启用规则的权限	写入	rule-on-custom-event-bus		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			rule-on-default-event-bus		
				events:creatorAccount events:ManagedBy	
InvokeApiDestination[仅权限]	授予调用 api 目标的权限	Write	api-destination*		
ListApiDestinations	授予检索 api 目标列表的权限	List			
ListArchives	授予检索存档列表的权限	List			
ListConnections	授予权限以检索连接列表	列表			
ListEndpoints	授予检索终端节点列表的权限	列表			
ListEventBuses	授予检索账户中事件总线列表的权限	列表			
ListEventSources	授予检索与此账户共享的事件源列表的权限	列表			
ListPartnerEventSourceAccounts	授予检索与事件源 Amazon Web Services 账户 IDs 关联的列表的权限	列表	event-source*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListPartnerEventSources	授予检索合作伙伴事件源列表的权限	List			
ListReplays	授予检索重播列表的权限	List			
ListRuleNamesByTarget	授予检索与目标关联的规则名称列表的权限	列表			
ListRules	授予在账户中检索亚马逊 EventBridge 规则列表的权限	列表			
ListTagsForResource	授予检索与 Amazon EventBridge 资源关联的标签列表的权限	列表	event-bus		
			rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount	
ListTargetsByRule	授予检索针对规则定义的目标列表的权限	列表	rule-on-custom-event-bus		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			rule-on-default-event-bus		
				events:creatorAccount	
PutEvents	授予向 Amazon 发送自定义事件的权限 EventBridge	写入	event-bus*		
				events:detail-type events:source events:eventBusInvocation	
PutPartnerEvents	授予向 Amazon 发送自定义事件的权限 EventBridge	写入			
PutPermission	授予使用该 PutPermission 操作的权限向其他人授予将事件放 Amazon Web Services 账户到您的默认事件总线的权限	权限管理			
PutRule	授予权限以创建或更新规则	写入	rule-on-custom-event-bus		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			rule-on-default-event-bus		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				events:detail.userIdentity.principalId events:detail-type events:source events:detail.service events:detail.eventTypeCode aws:RequestTag/${TagKey} aws:TagKeys events:creatorAccount events:ManagedBy	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutTargets	授予权限以向规则添加目标	写入	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:TargetArn events:creatorAccount events:ManagedBy	
RemovePermission	授予撤销他人将事件放 Amazon Web Services 账户 到您的默认事件总线的权限的权限	权限管理			
RemoveTargets	授予将目标从规则中删除的权限	写入	rule-on-custom-event-bus		
			rule-on-default-event-bus		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				events:creatorAccount events:ManagedBy	
RetrieveConnectionCredentials[仅权限]	授予检索来自连接的凭证的权限	写入	connection*		
StartReplay	授予启动存档重播的权限	写入	archive*		
			event-bus*		
			replay*		
TagResource	授予向 Amazon EventBridge 资源添加标签的权限	标记	event-bus		
			rule-on-custom-event-bus		
			rule-on-default-event-bus		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys aws:RequestTag/${TagKey} events:creatorAccount	
TestEventPattern	授予测试事件模式是否与提供的事件匹配的权限	读取			
UntagResource	授予从 Amazon EventBridge 资源中移除标签的权限	标记	event-bus		
			rule-on-custom-event-bus		
			rule-on-default-event-bus		
				aws:TagKeys events:creatorAccount	
UpdateApiDestination	授予更新 api 目标的权限	Write	api-destination*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateArchive	授予更新存档的权限	Write	archive*		
UpdateConnection	授予权限以更新连接	写入	connection*		
UpdateEndpoint	授予权限以更新终端节点	写入	endpoint*		
				events:EventBusArn	
UpdateEventBus	授予权限以更新事件总线	写入	event-bus*		

Amazon 定义的资源类型 EventBridge

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}

资源类型	ARN	条件键
rule-on-custom-event-bus	arn:${Partition}:events:${Region}:${Account}:rule/${EventBusName}/${RuleName}	aws:ResourceTag/${TagKey}
archive	arn:${Partition}:events:${Region}:${Account}:archive/${ArchiveName}	
replay	arn:${Partition}:events:${Region}:${Account}:replay/${ReplayName}	
connection	arn:${Partition}:events:${Region}:${Account}:connection/${ConnectionName}	
api-destination	arn:${Partition}:events:${Region}:${Account}:api-destination/${ApiDestinationName}	
endpoint	arn:${Partition}:events:${Region}:${Account}:endpoint/${EndpointName}	
create-snapshot	arn:${Partition}:events:${Region}:${Account}:target/create-snapshot	
reboot-instance	arn:${Partition}:events:${Region}:${Account}:target/reboot-instance	
stop-instance	arn:${Partition}:events:${Region}:${Account}:target/stop-instance	
terminate-instance	arn:${Partition}:events:${Region}:${Account}:target/terminate-instance	

Amazon 的条件密钥 EventBridge

Amazon EventBridge 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据每个标签的允许值集筛选对事件总线和规则操作的访问权限	字符串
aws:ResourceTag/${TagKey}	根据与资源关联的标签值筛选对事件总线和规则操作的访问权限	字符串
aws:TagKeys	按请求中的标签筛选对事件总线和规则操作的访问权限	ArrayOfString
events:EventBusArn	按可与终端节点关联的事件总线的 ARN 筛选访问权限和操作 CreateEndpoint UpdateEndpoint	ArrayOfARN
events:ManagedBy	按 Amazon 服务筛选访问权限。如果规则是由 Amazon 服务代表您创建的，则该值为创建该规则的服务的主体名称	字符串
events:TargetArn	按目标的 ARN 筛选访问权限，该目标可以应用于操作规则。 PutTargets targetArn 不包括 DeadLetterConfigArn	ArrayOfARN
events:creatorAccount	根据创建规则的账户筛选对规则操作的访问权限	字符串
events:detail-type	按事件的详细信息类型的文字字符串筛选访问权限和操作 PutEvents PutRule	字符串
events:detail.eventTypeCode	按字面字符串筛选访问权限以获取详细信息。 eventTypeCode 事件字段到 PutRule 操作	字符串
events:detail.service	按事件的 detail.service 字段的文字字符串筛选对操作的访问权限 PutRule	字符串
events:detail.userIdentity.principalId	按事件的 detail.useridentity.principalid 字段的文字字符串筛选对操作的访问权限 PutRule	字符串

条件键	描述	类型
events:eventBusInvocation	根据事件是通过 API 还是跨账户总线调用生成的，将访问权限筛选为操作 PutEvents	字符串
events:source	筛选生成事件的 Amazon 服务或 Amazon 合作伙伴事件源对 PutEvents 和 PutRule 操作的访问权限。匹配事件的 source 字段的文字字符串	ArrayOfString

Amazon 发票管理的操作、资源和条件键

Amazon 发票管理（服务前缀：`fapiao`）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon 发票管理定义的操作
- Amazon 发票管理定义的资源类型
- Amazon 发票管理的条件键

Amazon 发票管理定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用

Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetAccountFapiaoSetting	授予权限以获取账户发票设置	读取			
UpdateAccountFapiaoInformation	授予更新账户发票信息的权限	写入			

Amazon 发票管理定义的资源类型

Amazon 发票管理不支持在 IAM policy 语句的 Resource 元素中指定资源 ARN。要允许对 Amazon 发票管理的访问权限，请在策略中指定 "Resource": "*"。

Amazon 发票管理的条件键

发票没有可以在策略语句的 Condition 元素中使用的服务特定上下文键。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon 免费套餐的操作、资源和条件键

Amazon 免费套餐（服务前缀:freetier）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon 免费套餐定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetFreeTierAlertPreference[仅权限]	授予权限以获取免费套餐提醒首选项（通过电子邮件地址）	读取			
GetFreeTierUsage	授予权限以获取免费套餐使用限制和 MTD 使用状态	读取			
PutFreeTierAlertPreference[仅权限]	授予权限以设置免费套餐提醒首选项（通过电子邮件地址）	写入			

Amazon 免费套餐定义的资源类型

Amazon 免费套餐不支持在 IAM 政策声明的`Resource`元素中指定资源 ARN。要允许访问 Amazon 免费套餐，请在策略中指定 `"Resource": "*"`。

Amazon 免费套餐的条件键

免费套餐没有可以在策略语句的 `Condition` 元素中使用的服务特定上下文键。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon FreeRTOS 的操作、资源和条件键

Amazon FreeRTOS（服务前缀：`freertos`）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon FreeRTOS 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateSoftwareConfiguration	授予创建软件配置的权限	写入	configuration*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscription	授予创建 FreeRTOS 扩展维护计划 (EMP) 订阅的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSoftwareConfiguration	授予删除软件配置的权限	写入	configuration*		
DescribeHardwarePlatform	授予描述硬件平台的权限	读取			
DescribeSoftwareConfiguration	授予描述软件配置的权限	读取	configuration*		
DescribeSubscription	授予描述 FreeRTOS 扩展维护计划 (EMP) 订阅的权限	读取	subscription*		
GetEmpPatchUrl	授予权限以获取 FreeRTOS 扩展维护计划 (EMP) 下的软件补丁发布、补丁差异和发布说明的 URL	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetSoftwareURL	授予获取 Amazon FreeRTOS 软件下载 URL 的权限	读取			
GetSoftwareURLForConfiguration	授予根据配置获取 Amazon FreeRTOS 软件下载 URL 的权限	读取			
GetSubscriptionBillingAmount	授予获取 FreeRTOS 扩展维护计划 (EMP) 订阅计费金额的权限	读取			
ListFreeRTOSVersions	授予列出 AmazonFree RTOS 版本的权限	列表			
ListHardwarePlatforms	授予列出硬件平台的权限	列表			
ListHardwareVendors	授予列出硬件供应商的权限	列表			
ListSoftwareConfigurations	授予列出软件配置的权限	列表			
ListSoftwarePatches	授予列出 FreeRTOS 扩展维护计划 (EMP) 订阅软件补丁的权限	列表			
ListSubscriptionEmails	授予列出 FreeRTOS 扩展维护计划 (EMP) 订阅电子邮件的权限	列表			
ListSubscriptions	授予列出 FreeRTOS 扩展维护计划 (EMP) 订阅的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateEmailRecipients	授予更新 FreeRTOS 扩展维护计划 (EMP) 订阅电子邮件地址列表的权限	写入			
UpdateSoftwareConfiguration	授予更新软件配置的权限	写入	configuration*		
VerifyEmail	授予验证 FreeRTOS 扩展维护计划 (EMP) 电子邮件的权限	写入			

Amazon FreeRTOS 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
configuration	arn:${Partition}:freertos:${Region}:${Account}:configuration/${ConfigurationName}	aws:ResourceTag/${TagKey}
subscription	arn:${Partition}:freertos:${Region}:${Account}:subscription/${SubscriptionID}	aws:ResourceTag/${TagKey}

Amazon FreeRTOS 的条件键

Amazon FreeRTOS 定义以下可以在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按用户向 Amazon FreeRTOS 发出的请求中包含的标签键筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按附加到 Amazon FreeRTOS 资源的标签键组件筛选访问权限	字符串
aws:TagKeys	按与请求中的资源关联的所有标签键名称的列表筛选访问	ArrayOfString

Amazon 的操作、资源和条件密钥 FSx

Amazon FSx （服务前缀:fsx）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon 定义的操作 FSx
- Amazon 定义的资源类型 FSx
- Amazon 的条件密钥 FSx

Amazon 定义的操作 FSx

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，

以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateFileGateway[仅权限]	授予将文件网关实例与 Amazon for Window FSx s 文件服务器文件系统关联的权限	写入	file-system*		
AssociateFileSystemAliases	授予将 DNS 别名与 Windows 版亚马逊文件服务器文件系统关联 FSx 的权限	写入	file-system*		
BypassSnaplockEnterpriseRetention[仅权限]	授予允许删除包含 WORM（一次写入，多次读取）且保留期处于活动状态的 ONTAP En SnapLock terprise 卷的权限 FSx	权限管理	volume*		
CancelDataRepositoryTask	授予取消数据存储库任务的权限	Write	task*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CopyBackup	授予复制备份的权限	写入	backup*		fsx:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CopySnapshotAndUpdateVolume	授予使用来自其他 Amazon for OpenZFS 文件系统的快照来更新现有卷 FSx 的权限	写入	snapshot*		
			volume*		
CreateBackup	授予创建亚马逊 FSx 文件系统或亚马逊 FSx 卷新备份的权限	写入	backup*		fsx:TagResource
			file-system		
			volume		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataRepositoryAssociation	授予为 Amazon for Lustre 文件系统创建新的数据存储库关联 FSx 的权限	写入	association*		fsx:TagResource
			file-system*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataRepositoryTask	授予为 Amazon for Lustre 文件系统创建新数据存储库任务 FSx 的权限	写入	file-system*		fsx:TagResource
			task*		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateFileCache	授予创建新的空 Amazon 文件缓存的权限	写入	file-cache*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:GetSecurityGroupsForVpc fsx:CreateDataRepositoryAssociation fsx:TagResource logs:CreateLogGroup logs:CreateLogStream logs:PutLogEvents

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
					s3:ListBucket
			association	fsx:NfsDataRepositoryEncryptionInTransitEnabled fsx:NfsDataRepositoryAuthenticationEnabled	
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFileSystem	授予创建新的、空的 Amazon FSx 文件系统的权限	写入	file-system*		ec2:GetSecurityGroupsForVpc fsx:TagResource

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFileSystemFromBackup	授予使用现有备份创建新 Amazon FSx 文件系统的权限	写入	backup*		ec2:GetSecurityGroupsForVpc fsx:TagResource
			file-system*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshot	授予权限以在卷上创建新快照	写入	snapshot*		fsx:TagResource
			volume*		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateStorageVirtualMachine	授予在 Amazon FSx for Ontap 文件系统中创建新存储虚拟机的权限	写入	file-system*		fsx:TagResource
			storage-virtual-machine*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVolume	授予权限以新建卷	写入	volume*		fsx:TagResource
			snapshot		
				aws:RequestTag/${TagKey} aws:TagKeys fsx:StorageVirtualMachineId fsx:ParentVolumeId	
CreateVolumeFromBackup	授予权限以创建新的备份卷	写入	backup*		fsx:TagResource

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			storage-virtual-machine*		
			volume*		
				aws:RequestTag/${TagKey} aws:TagKeys fsx:StorageVirtualMachineId	
DeleteBackup	授予权限以删除备份，从而删除其内容。在删除后，备份不再存在并且其数据不再可用	写入	backup*		
DeleteDataRepositoryAssociation	授予权限以删除数据存储库关联	写入	association*		
DeleteFileCache	授予删除文件缓存、删除其内容的权限	写入	file-cache*		fsx:DeleteDataRepositoryAssociation
			association		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFileSystem	授予删除文件系统，从而删除其内容以及文件系统的任何现有自动备份的权限	写入	file-system*		fsx:CreateBackup fsx:TagResource
			backup		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteResourcePolicy[仅权限]	需要通过 Amazon 资源访问管理器 (RAM) 管理 FSx 卷的跨账户共享。 PutResourcePolicy 而且 GetResourcePolicy 也是必需的	权限管理	volume*		
DeleteSnapshot	授予权限以删除卷上的快照	写入	snapshot*		
DeleteStorageVirtualMachine	授予删除存储虚拟机以删除其内容的权限	写入	storage-virtual-machine*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteVolume	授予删除卷以及删除其内容和卷的任何现有自动备份的权限	写入	volume*		fsx:TagResource
			backup		
				aws:RequestTag/${TagKey} aws:TagKeys fsx:StorageVirtualMachineId fsx:ParentVolumeId	
DescribeAssociatedFileGateways[仅权限]	授予描述与 Amazon for Windows 文件服务器文件系统关联的文件网关实例 FSx 的权限	读取	file-system*		
DescribeBackups	授予在您调用的终端节点 Amazon Web Services 账户 中返回您拥有的所有备份描述 Amazon Web Services 区域 的权限	读取			
DescribeDataRepositoryAssociations	授予在你正在调用的终端节点 Amazon Web Services 账户 中返回你拥有的所有数据存储库关联描述 Amazon Web Services 区域 的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeDataRepositoryTasks	授予在你正在调用的终端节点 Amazon Web Services 账户 中返回你拥有的所有数据存储库任务描述 Amazon Web Services 区域 的权限	读取			
DescribeFileCaches	授予在你正在调用的终端节点 Amazon Web Services 账户 中返回你拥有的所有文件缓存描述 Amazon Web Services 区域 的权限	读取			
DescribeFileSystemAliases	授予返回您的 Amazon for Windows 文件服务器文件系统所拥有 FSx 的所有 DNS 别名的描述的权限	读取	file-system*		
DescribeFileSystems	授予在你正在调用的终端节点 Amazon Web Services 账户 中返回你拥有的所有文件系统的描述 Amazon Web Services 区域 的权限	读取			
DescribeSharedVpcConfiguration	授予返回您的账户中是否允许从参与者账户更新 FSx 路由表的描述的权限	读取			
DescribeSnapshots	授予在你正在调用的终端节点 Amazon Web Services 账户 中返回你拥有的所有快照 Amazon Web Services 区域 的描述的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeStorageVirtualMachines	授予在您调用的终端节点 Amazon Web Services 账户 中返回您拥有的所有存储虚拟机的描述 Amazon Web Services 区域 的权限	读取			
DescribeVolumes	授予在你正在调用的终端节点 Amazon Web Services 账户 中返回你拥有的所有卷描述 Amazon Web Services 区域 的权限	读取			
DisassociateFileGateway[仅权限]	授予取消文件网关实例与 Amazon for Windows 文件服务器文件系统的关联 FSx 的权限	写入	file-system*		
DisassociateFileSystemAliases	授予取消文件系统别名与 Amazon for Windows 文件服务器文件系统的关联 FSx 的权限	写入	file-system*		
GetResourcePolicy[仅权限]	需要通过 Amazon 资源访问管理器 (RAM) 管理 FSx 卷的跨账户共享。 PutResourcePolicy 而且 DeleteResourcePolicy 也是必需的	权限管理	volume*		
ListTagsForResource	授予列出 Amazon FSx 资源标签的权限	读取	association		
			backup		
			file-cache		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			file-system		
			snapshot		
			storage-virtual-machine		
			task		
			volume		
ManageBackupPrincipalAssociations[仅权限]	授予通过 Amazon Backup 管理备份主体关联的权限	权限管理	backup*		
PutResourcePolicy[仅权限]	需要通过 Amazon 资源访问管理器 (RAM) 管理 FSx 卷的跨账户共享。 DeleteResourcePolicy 而且 GetResourcePolicy 也是必需的	权限管理	volume*		
ReleaseFileSystemNfsV3Locks	授予解除文件系统 NFS V3 锁的权限	写入	file-system*		
RestoreVolumeFromSnapshot	授予从快照恢复卷状态的权限	写入	snapshot*		
			volume*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StartMisconfiguredStateRecovery	授予权限以启动配置错误的状态恢复	写入	file-system*		
TagResource	授予标记 Amazon FSx 资源的权限	标记	association		
			backup		
			file-cache		
			file-system		
			snapshot		
			storage-virtual-machine		
			task		
			volume		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	授予从 Amazon FSx 资源中移除标签的权限	标记	association		
			backup		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			file-cache		
			file-system		
			snapshot		
			storage-virtual-machine		
			task		
			volume		
				aws:TagKeys	
UpdateDataRepositoryAssociation	授予权限以更新数据存储库关联配置	写入	association*		
UpdateFileCache	授予更新文件缓存配置的权限	写入	file-cache*		
UpdateFileSystem	授予权限以更新文件系统的配置	写入	file-system*		
UpdateSharedVpcConfiguration	授予权限以启用或禁用您账户中参与者账户的 FSx 路由表更新	写入			
UpdateSnapshot	授予权限以更新快照配置	写入	snapshot*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateStorageVirtualMachine	授予权限以更新存储虚拟机配置	写入	storage-virtual-machine*		
UpdateVolume	授予权限以更新卷配置	写入	volume*		
				fsx:StorageVirtualMachineId fsx:ParentVolumeId	

Amazon 定义的资源类型 FSx

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

> **Note**
>
> FSx 适用于 Windows 的亚马逊文件服务器、Lustre 和 Ontap 共享一些相同的资源类型，每种资源类型的 ARN 格式相同。

资源类型	ARN	条件键
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}

资源类型	ARN	条件键
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}

Amazon 的条件密钥 FSx

Amazon FSx 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串

条件键	描述	类型
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString
fsx:IsBackupCopyDestination	根据备份是否为 CopyBackup 操作的目标备份来筛选访问权限	布尔型
fsx:IsBackupCopySource	根据备份是否为 CopyBackup 操作的源备份来筛选访问权限	布尔型
fsx:NfsDataRepositoryAuthenticationEnabled	按支持身份验证的 NFS 数据存储库筛选访问	布尔型
fsx:NfsDataRepositoryEncryptionInTransitEnabled	按支持的 NFS 数据存储库筛选访问权限 encryption-in-transit	布尔型
fsx:ParentVolumeId	按包含父级卷筛选访问权限，以便改变卷操作	字符串
fsx:StorageVirtualMachineId	筛选包含存储虚拟机对卷的访问权限，以便改变卷操作	字符串

Amazon 的操作、资源和条件密钥 GameLift

Amazon GameLift （服务前缀:`gamelift`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon 定义的操作 GameLift
- Amazon 定义的资源类型 GameLift
- Amazon 的条件密钥 GameLift

Amazon 定义的操作 GameLift

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AcceptMatch	授予注册玩家接受或拒绝提议的 FlexMatch 比赛的权限	写入			
ClaimGameServer	授予权限以查找并保留游戏服务器来托管新的游戏会话	Write	gameServerGroup*		
CreateAlias	授予权限以为队组定义新别名	Write		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreateBuild	授予权限以使用存储在 Amazon S3 存储桶中的文件创建新的游戏生成包	写入		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource iam:PassRole s3:GetObject
CreateContainerFleet	授予创建新的计算资源容器队列以运行游戏服务器的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeAvailabilityZones ec2:DescribeRegions gamelift:TagResource

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
					iam:PassRole
CreateContainerGroupDefinition	授予使用存储在 Amazon ECR 存储库中的图像创建新的容器组定义的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	ecr:BatchGetImage ecr:DescribeImages ecr:GetAuthorizationToken ecr:GetDownloadUrlForLayer gamelift:TagResource

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateFleet	授予权限以创建新的计算资源队组来运行您的游戏服务器	Write		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeAvailabilityZones ec2:DescribeRegions gamelift:TagResource iam:PassRole
CreateFleetLocations	授予权限以为队组指定其他位置	Write	containerFleet		ec2:DescribeAvailabilityZones ec2:DescribeRegions
			fleet		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateGameServerGroup	授予权限以创建新的游戏服务器组，设置相应的 Auto Scaling 组并启动实例以托管游戏服务器	Write		aws:RequestTag/${TagKey} aws:TagKeys	autoscaling:CreateAutoScalingGroup autoscaling:DescribeAutoScalingGroups autoscaling:PutLifecycleHook autoscaling:PutScalingPolicy ec2:DescribeAvailabilityZones ec2:DescribeSubnets events:PutRule events:PutTargets

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
					gamelift:TagResource iam:PassRole
CreateGameSession	授予权限以在指定队组上启动新的游戏会话	Write			
CreateGameSessionQueue	授予权限以设置新队组来处理游戏会话放置请求	写入		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreateLocation	授予权限以为实例集定义新位置	写入		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreateMatchmakingConfiguration	授予创建新 FlexMatch 媒人的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateMatchmakingRuleSet	授予权限以创建新的配对规则集 FlexMatch	写入		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreatePlayerSession	授予权限以为一个玩家保留可用的游戏会话位置	Write			
CreatePlayerSessions	授予权限以为多个玩家保留可用的游戏会话位置	Write			
CreateScript	授予创建新的 Realtime Servers 脚本的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource iam:PassRole s3:GetObject

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateVpcPeeringAuthorization	授予 GameLift 允许在 GameLift 队列 VPC 与另一个 VPC 上的 VPC 之间创建或删除对等连接的权限 Amazon Web Services 账户	写入			ec2:AcceptVpcPeeringConnection ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateRoute ec2:DeleteRoute ec2:DescribeRouteTables ec2:DescribeSecurityGroups ec2:RevokeSecurityGroupEgress

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
					ec2:RevokeSecurityGroupIngress
CreateVpcPeeringConnection	授予在您的 GameLift 队列 VPC 与其他账户上的 VPC 之间建立对等连接的权限	写入			
DeleteAlias	授予权限以删除别名	Write	alias*		
DeleteBuild	授予权限以删除游戏生成包	写入	build*		
DeleteContainerFleet	授予删除集装箱舰队的权限	写入	containerFleet*		
DeleteContainerGroupDefinition	授予删除容器组定义的权限	写入	containerGroupDefinition*		
DeleteFleet	授予权限以删除空队组	Write	fleet*		
DeleteFleetLocations	授予权限以删除队组位置	Write	containerFleet		
			fleet		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteGameServerGroup	授予权限以永久删除游戏服务器组并终止相应 Auto Scaling 组的 FleetIQ 活动	Write	gameServerGroup*		autoscaling:DeleteAutoScalingGroup autoscaling:DescribeAutoScalingGroups autoscaling:ExitStandby autoscaling:ResumeProcesses autoscaling:SetInstanceProtection autoscaling:UpdateAutoScalingGroup
DeleteGameSessionQueue	授予权限以删除现有游戏会话队列	写入	gameSessionQueue*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteLocation	授予权限以删除位置	写入	location*		
DeleteMatchmakingConfiguration	授予删除现有 FlexMatch 媒人的权限	写入	matchmakingConfiguration*		
DeleteMatchmakingRuleSet	授予删除现有 FlexMatch 配对规则集的权限	写入	matchmakingRuleSet*		
DeleteScalingPolicy	授予权限以删除一组自动伸缩规则	Write	containerFleet		
			fleet		
DeleteScript	授予权限以删除 Realtime Servers 脚本	Write	script*		
DeleteVpcPeeringAuthorization	授予权限以取消 VPC 对等授权	写入			
DeleteVpcPeeringConnection	授予移除之间的对等连接的权限 VPCs	写入			
DeregisterCompute	授予权限以对实例集取消注册计算	写入	fleet*		
DeregisterGameServer	授予权限以从游戏服务器组中删除游戏服务器	Write	gameServerGroup*		
DescribeAlias	授予权限以检索别名属性	Read	alias*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeBuild	授予权限以检索游戏生成包属性	读取	build*		
DescribeCompute	授予检索队列中计算信息的权限	读取	containerFleet		
			fleet		
DescribeContainerFleet	授予检索现有集装箱舰队属性的权限	读取	containerFleet*		
DescribeContainerGroupDefinition	授予检索现有容器组定义属性的权限	读取	containerGroupDefinition*		
DescribeEC2InstanceLimits	授予检索 EC2 实例类型允许的最大使用量和当前使用量的权限	读取			
DescribeFleetAttributes	授予权限以检索队组的常规属性，包括状态	读取			
DescribeFleetCapacity	授予检索托管舰队当前容量设置的权限	读取			
DescribeFleetDeployment	授予检索现有舰队部署属性的权限	读取	containerFleet*		
DescribeFleetEvents	授予权限以从队组的事件日志中检索条目	Read	containerFleet		
			fleet		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeFleetLocationAttributes	授予权限以检索队组位置的常规属性，包括状态	Read	containerFleet		
			fleet		
DescribeFleetLocationCapacity	授予权限以检索队组位置的当前容量设置	Read	containerFleet		
			fleet		
DescribeFleetLocationUtilization	授予权限以检索队组位置的利用率统计信息	Read	fleet*		
DescribeFleetPortSettings	授予权限以检索队组的入站连接权限	Read	fleet*		
DescribeFleetUtilization	授予权限以检索队组的利用率统计信息	Read			
DescribeGameServer	授予权限以检索游戏服务器的属性	Read	gameServerGroup*		
DescribeGameServerGroup	授予权限以检索游戏服务器组的属性	读取	gameServerGroup*		
DescribeGameServerInstances	授予检索游戏服务器组中 EC2 实例状态的权限	读取	gameServerGroup*		
DescribeGameSessionDetails	授予权限以检索队组中游戏会话的属性，包括保护策略	Read			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeGameSessionPlacement	授予权限以检索游戏会话放置请求的详细信息	Read			
DescribeGameSessionQueues	授予权限以检索游戏会话队列的属性	Read			
DescribeGameSessions	授予权限以检索队组中游戏会话的属性	读取			
DescribeInstances	授予检索托管队列中实例信息的权限	读取	containerFleet		
			fleet		
DescribeMatchmaking	授予权限以检索对战门票的详细信息	读取			
DescribeMatchmakingConfigurations	授予 FlexMatch 媒人检索房产的权限	读取			
DescribeMatchmakingRuleSets	授予检索 FlexMatch 配对规则集属性的权限	读取			
DescribePlayerSessions	授予权限以检索游戏会话中玩家会话的属性	Read			
DescribeRuntimeConfiguration	授予权限以检索队组的当前运行配置	Read	fleet*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeScalingPolicies	授予权限以检索应用于队组的所有伸缩策略	Read	containerFleet		
			fleet		
DescribeScript	授予权限以检索 Realtime Servers 脚本的属性	Read	script*		
DescribeVpcPeeringAuthorizations	授予权限以检索有效的 VPC 对等授权	Read			
DescribeVpcPeeringConnections	授予权限以检索活动或待处理 VPC 对等连接的详细信息	读取			
GetComputeAccess	授予检索证书的权限，以远程访问托管队列中的计算机	读取	containerFleet		
			fleet		
GetComputeAuthToken	授予检索身份验证令牌的权限，该令牌允许计算机上的进程向 Amazon GameLift 服务发送请求	读取	containerFleet		
			fleet		
GetGameSessionLogUrl	授予权限以检索游戏会话的存储日志位置	Read			
GetInstanceAccess	授予权限以请求远程访问指定队组实例	Read	fleet*		
ListAliases	授予权限以检索当前区域中定义的所有别名	List			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListBuilds	授予权限以检索当前区域中的所有游戏生成包	列表			
ListCompute	授予权限以检索当前区域中的所有计算资源	列表	containerFleet		
			fleet		
ListContainerFleets	授予检索当前区域中所有现有集装箱舰队属性的权限	列表			
ListContainerGroupDefinitionVersions	授予检索现有容器组定义所有版本属性的权限	列表	containerGroupDefinition*		
ListContainerGroupDefinitions	授予检索当前区域中所有现有容器组定义属性的权限	列表			
ListFleetDeployments	授予检索当前区域中所有现有舰队部署属性的权限	列表			
ListFleets	授予检索当前区域内所有舰队 IDs 的舰队列表的权限	列表			
ListGameServerGroups	授予权限以检索当前区域中定义的所有游戏服务器组	List			
ListGameServers	授予权限以检索当前在游戏服务器组中运行的所有游戏服务器	列表	gameServerGroup*		
ListLocations	授予权限以检索此账户中的所有位置	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListScripts	授予权限以检索当前区域中所有 Realtime Servers 脚本的属性	列表			
ListTagsForResource	授予检索 GameLift 资源标签的权限	读取	alias		
			build		
			containerFleet		
			containerGroupDefinition		
			fleet		
			gameServerGroup		
			gameSessionQueue		
			location		
			matchmakingConfiguration		
			matchmakingRuleSet		
			script		
PutScalingPolicy	授予权限以创建或更新队组自动伸缩策略	写入	containerFleet		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			fleet		
RegisterCompute	授予权限以对实例集注册计算	写入	fleet*		
RegisterGameServer	允许在新游戏服务器 GameLift 准备好托管游戏时通知 FleetIQ	写入	gameServerGroup*		
RequestUploadCredentials	授予权限以检索在上传新游戏生成包时使用的全新上传凭证	Read	build*		
ResolveAlias	授予权限以检索与别名关联的队组 ID	Read	alias*		
ResumeGameServerGroup	授予权限以恢复游戏服务器组的暂停 FleetIQ 活动	Write	gameServerGroup*		
SearchGameSessions	授予权限以检索匹配一组搜索标准的游戏会话	读取			
StartFleetActions	使用 StopFleetActions () 授予在队列暂停后恢复其自动缩放活动的权限	写入	containerFleet		
			fleet		
StartGameSessionPlacement	授予权限以向游戏会话队列发送游戏会话放置请求	写入	gameSessionQueue*		
StartMatchBackfill	授予请求 FlexMatch 配对以填补现有游戏会话中可用玩家位置的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StartMatchmaking	授予为一个或一组玩家请求 FlexMatch 配对并启动游戏会话放置的权限	写入			
StopFleetActions	授予权限以暂停队组的自动伸缩活动	Write	containerFleet		
			fleet		
StopGameSessionPlacement	授予权限以取消正在进行的游戏会话放置请求	Write			
StopMatchmaking	授予权限以取消正在进行的对战匹配或对战回填请求	Write			
SuspendGameServerGroup	授予权限以暂时停止游戏服务器组的 FleetIQ 活动	写入	gameServerGroup*		
TagResource	授予标记 GameLift 资源的权限	标记	alias		
			build		
			containerFleet		
			containerGroupDefinition		
			fleet		
			gameServerGroup		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			gameSessionQueue		
			location		
			matchmakingConfiguration		
			matchmakingRuleSet		
			script		
				aws:RequestTag/${TagKey} aws:TagKeys	
TerminateGameSession	授予关闭现有游戏会话的权限	写入			
UntagResource	授予取消标记资源的 GameLift 权限	标记	alias		
			build		
			containerFleet		
			containerGroupDefinition		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			fleet		
			gameServerGroup		
			gameSessionQueue		
			location		
			matchmakingConfiguration		
			matchmakingRuleSet		
			script		
				aws:TagKeys	
UpdateAlias	授予权限以更新现有别名的属性	Write	alias*		
UpdateBuild	授予权限以更新现有生成包的元数据	写入	build*		
UpdateContainerFleet	授予更新现有集装箱舰队的权限	写入	containerFleet*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateContainerGroupDefinition	授予更新现有容器组定义属性的权限	写入	containerGroupDefinition*		ecr:BatchGetImage ecr:DescribeImages ecr:GetAuthorizationToken ecr:GetDownloadUrlForLayer
UpdateFleetAttributes	授予权限以更新现有队组的常规属性	写入	fleet*		
UpdateFleetCapacity	授予调整托管队列容量设置的权限	写入	containerFleet		
			fleet		
UpdateFleetPortSettings	授予权限以调整队组的端口设置	Write	fleet*		
UpdateGameServer	授予权限以更改游戏服务器属性、运行状况或利用率状态	Write	gameServerGroup*		
UpdateGameServerGroup	授予权限以更新游戏服务器组的属性，包括允许的实例类型	Write	gameServerGroup*		iam:PassRole
UpdateGameSession	授予权限以更新现有游戏会话的属性	Write			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateGameSessionQueue	授予权限以更新现有游戏会话队列的属性	写入	gameSessionQueue*		
UpdateMatchmakingConfiguration	授予更新现有 FlexMatch 配对配置属性的权限	写入	matchmakingConfiguration*		
UpdateRuntimeConfiguration	授予权限以更新如何在现有队组的实例上配置服务器进程	Write	fleet*		
UpdateScript	授予权限以更新现有 Realtime Servers 脚本的元数据和内容	写入	script*		iam:PassRole s3:GetObject
ValidateMatchmakingRuleSet	授予验证 FlexMatch 配对规则集语法的权限	读取			

Amazon 定义的资源类型 GameLift

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
alias	`arn:${Partition}:gamelift:${Region}::alias/${AliasId}`	aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
build	arn:${Partition}:gamelift:${Region}:${Account}:build/${BuildId}	aws:ResourceTag/${TagKey}
containerGroupDefinition	arn:${Partition}:gamelift:${Region}:${Account}:containergroupdefinition/${Name}	aws:ResourceTag/${TagKey}
containerFleet	arn:${Partition}:gamelift:${Region}:${Account}:containerfleet/${FleetId}	aws:ResourceTag/${TagKey}
fleet	arn:${Partition}:gamelift:${Region}:${Account}:fleet/${FleetId}	aws:ResourceTag/${TagKey}
gameServerGroup	arn:${Partition}:gamelift:${Region}:${Account}:gameservergroup/${GameServerGroupName}	aws:ResourceTag/${TagKey}
gameSessionQueue	arn:${Partition}:gamelift:${Region}:${Account}:gamesessionqueue/${GameSessionQueueName}	aws:ResourceTag/${TagKey}
location	arn:${Partition}:gamelift:${Region}:${Account}:location/${LocationId}	aws:ResourceTag/${TagKey}
matchmakingConfiguration	arn:${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}

Amazon 的条件密钥 GameLift

Amazon GameLift 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString

Amazon Glue 的操作、资源和条件键

Amazon Glue（服务前缀:glue）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Glue 定义的操作
- Amazon Glue 定义的资源类型
- Amazon Glue 的条件键

Amazon Glue 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AuthorizeInboundIntegration[仅权限]	向 Glue 授予持续验证目标 Arn 是否可以接收从源 ARN 复制的数据的权限	写入	integration*		
BatchCreatePartition	授予权限以创建一个或多个分区	Write	database*		
			rootcatalog*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			table*		
			catalog		
BatchDeleteConnection	授予权限以删除一个或多个连接	Write	connection*		
			rootcatalog*		
BatchDeletePartition	授予权限以删除一个或多个分区	Write	database*		
			rootcatalog*		
			table*		
			catalog		
BatchDeleteTable	授予权限以删除一个或多个表	Write	database*		
			rootcatalog*		
			table*		
			catalog		
BatchDeleteTableVersion	授予权限以删除表的一个或多个版本	写入	database*		
			rootcatalog*		
			table*		
			catalog		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchGetBlueprints	授予权限以检索一个或多个蓝图	读取	blueprint*		
BatchGetCrawlers	授予权限以检索一个或多个爬网程序	读取	crawler*		
BatchGetCustomEntityTypes	授予权限以检索一个或多个自定义实体类型	读取			
BatchGetDevEndpoints	授予权限以检索一个或多个开发终端节点	Read	devendpoint*		
BatchGetJobs	授予权限以检索一个或多个作业	Read	job*		
BatchGetPartition	授予权限以检索一个或多个分区	读取	database*		
			rootcatalog*		
			table*		
			catalog		
BatchGetStageFiles	授予权限以批量获取 SparkUI 的阶段文件	权限管理			
BatchGetTableOptimizer	授予返回指定的表优化器配置的权限	读取	database*		glue:GetTable
			rootcatalog*		
			table*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchGetTriggers	授予权限以检索一个或多个触发器	Read	trigger*		
BatchGetWorkflows	授予权限以检索一个或多个工作流程	Read	workflow*		
BatchStopJobRun	授予权限以停止作业的一个或多个作业运行	写入	job*		
BatchUpdatePartition	授予权限以更新一个或多个分区	写入	database*		
			rootcatalog*		
			table*		
			catalog		
CancelDataQualityRuleRecommendationRun	授予权限以停止正在运行的数据质量规则建议运行	写入	dataQualityRuleset*		
CancelDataQualityRulesetEvaluationRun	授予权限以停止正在运行的数据质量规则集评估运行	写入	dataQualityRuleset*		
CancelMLTaskRun	授予权限以停止正在运行的 ML 任务运行	写入	mlTransform*		
CancelStatement	授予权限以取消交互式会话中的语句	写入	session*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CheckSchemaVersionValidity	授予检索架构版本有效性检查的权限	读取			
CreateBlueprint	授予权限以创建蓝图	写入	blueprint*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCatalog	授予创建目录的权限	写入	catalog*		
			rootcatalog*		
CreateClassifier	授予权限以创建分类器	写入			
CreateColumnStatisticsTaskSettings	授予为列统计任务创建设置的权限	写入	database*		
			rootcatalog*		
			table*		
CreateConnection	授予权限以创建连接	Write	rootcatalog*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCrawler	授予权限以创建爬网程序	写入		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomEntityType	授予权限以创建自定义实体类型	写入		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataQualityRuleset	授予权限以创建数据质量规则集	写入		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDatabase	授予权限以创建数据库	Write	database*		
			rootcatalog*		
			catalog		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateDevEndpoint	授予权限以创建开发终端节点	写入		aws:RequestTag/${TagKey} aws:TagKeys	
CreateInboundIntegration[仅权限]	向源委托人授予权限，允许其创建入站集成，以便将数据从源复制到目标	写入			
CreateIntegration	授予创建集成的权限	写入	catalog*		kms:CreateGrant kms:DescribeKey
			connection*		
			database*		
			integration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIntegrationResourceProperty	授予创建集成资源属性的权限	写入	catalog*		
			connection*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			database*		
CreateIntegrationTableProperties	授予创建集成表属性的权限	写入	catalog*		
			connection*		
			database*		
CreateJob	授予权限以创建作业	Write	job*		
				aws:RequestTag/${TagKey} aws:TagKeys glue:VpcIds glue:SubnetIds glue:SecurityGroupIds	
CreateMLTransform	授予权限以创建 ML 转换	Write		aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreatePartition	授予权限以创建分区	写入	database*		
			rootcatalog*		
			table*		
			catalog		
CreatePartitionIndex	授予权限以在现有表中创建指定的分区索引	写入	database*		
			rootcatalog*		
			table*		
			catalog		
CreateRegistry	授予创建新架构注册表的权限	Write	registry*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSchema	授予创建新架构容器的权限	Write	registry*		
			schema*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateScript	授予权限以创建脚本	Write			
CreateSecurityConfiguration	授予权限以创建安全配置	写入			
CreateSession	授予创建交互式会话的权限	写入	session*		
				aws:RequestTag/${TagKey} aws:TagKeys glue:VpcIds glue:SubnetIds glue:SecurityGroupIds	
CreateTable	授予权限以创建表	写入	database*		
			rootcatalog*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			table*		
			catalog		
CreateTableOptimizer	授予对特定函数创建新表优化器的权限。压缩是目前唯一支持的优化器类型	写入	database*		glue:GetTable
			rootcatalog*		
			table*		
CreateTrigger	授予权限以创建触发器	写入	trigger*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUsageProfile	授予权限以创建使用情况配置文件	写入	usageProfile*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUserDefinedFunction	授予权限以创建函数定义	Write	database*		
			rootcatalog*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			catalog		
CreateWorkflow	授予权限以创建工作流程	写入	workflow*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBlueprint	授予权限以删除蓝图	写入	blueprint*		
DeleteCatalog	授予删除目录的权限	写入	rootcatalog*		
			catalog		
DeleteClassifier	授予权限以删除分类器	写入			
DeleteColumnStatisticsForPartition	授予权限以删除列的分区列统计数据信息	写入	database*		
			rootcatalog*		
			table*		
			catalog		
DeleteColumnStatisticsForTable	授予删除列的表统计信息的权限	写入	database*		
			rootcatalog*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			table*		
			catalog		
DeleteColumnStatisticsTaskSettings	授予删除列统计任务设置的权限	写入	database*		
			rootcatalog*		
			table*		
DeleteConnection	授予权限以删除连接	Write	connection*		
			rootcatalog*		
DeleteCrawler	授予权限以删除爬网程序	写入	crawler*		
DeleteCustomEntityType	授予权限以删除自定义实体类型	写入			
DeleteDataQualityRuleset	授予权限以删除数据质量规则集	写入	dataQualityRuleset*		
DeleteDatabase	授予权限以删除数据库	Write	database*		
			rootcatalog*		
			table*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			userdefinedfunction*		
			catalog		
DeleteDevEndpoint	授予权限以删除开发终端节点	写入	devendpoint*		
DeleteIntegration	授予删除集成的权限	写入	integration*		
				aws:ResourceTag/${TagKey}	
DeleteIntegrationTableProperties	授予删除集成表属性的权限	写入	catalog*		
			connection*		
			database*		
DeleteJob	授予权限以删除作业	Write	job*		
DeleteMLTransform	授予权限以删除 ML 转换	Write	mlTransform*		
DeletePartition	授予权限以删除分区	写入	database*		
			rootcatalog*		
			table*		
			catalog		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeletePartitionIndex	授予权限以从现有表中删除指定的分区索引	写入	database*		
			rootcatalog*		
			table*		
			catalog		
DeleteRegistry	授予删除架构注册表的权限	Write	registry*		
DeleteResourcePolicy	授予权限以删除资源策略	Permissions management	rootcatalog*		
DeleteSchema	授予删除架构容器的权限	Write	registry*		
			schema*		
DeleteSchemaVersions	授予删除一系列架构版本的权限	Write	registry*		
			schema*		
DeleteSecurityConfiguration	授予权限以删除安全配置	写入			
DeleteSession	授予在停止交互式会话后删除交互式会话的权限（如果尚未停止）	写入	session*		
DeleteTable	授予权限以删除表	写入	database*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			rootcatalog*		
			table*		
			catalog		
DeleteTableOptimizer	授予删除表的一个优化器以及所有相关元数据的权限。将不再对该表执行优化	写入	database*		glue:GetTable
			rootcatalog*		
			table*		
DeleteTableVersion	授予权限以删除表版本	Write	database*		
			rootcatalog*		
			table*		
			catalog		
DeleteTrigger	授予权限以删除触发器	写入	trigger*		
DeleteUsageProfile	授予权限以删除用户配置文件	写入	usageProfile*		
DeleteUserDefinedFunction	授予权限以删除函数定义	Write	database*		
			rootcatalog*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			userdefinedfunction*		
			catalog		
DeleteWorkflow	授予权限以删除工作流程	写入	workflow*		
DeregisterDataPreview	授予权限以终止 Glue Studio 笔记本会话	权限管理			
DescribeConnectionType	授予权限以在 Glue Studio 中描述连接	权限管理			
DescribeEntity	授予权限以在 Glue Studio 中描述实体	权限管理	connection*		
			rootcatalog*		
DescribeInboundIntegrations	授予列出入站集成的权限	列表			
DescribeIntegrations	授予描述零 ETL 集成的权限	列表	integration*		
				aws:ResourceTag/${TagKey}	
GetBlueprint	授予权限以检索蓝图	读取	blueprint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetBlueprintRun	授予权限以检索蓝图运行	读取	blueprint*		
GetBlueprintRuns	授予权限以检索蓝图的所有运行	读取	blueprint*		
GetCatalog	授予检索目录的权限	读取	rootcatalog*		
			catalog		
				glue:EnabledForRedshiftAutoDiscovery	
GetCatalogImportStatus	授予权限以检索目录导入状态	读取	rootcatalog*		
GetCatalogs	授予检索所有目录的权限	读取	rootcatalog*		
			catalog		
				glue:EnabledForRedshiftAutoDiscovery	
GetClassifier	授予权限以检索分类器	Read			
GetClassifiers	授予权限以列出所有分类器	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetColumnStatisticsForPartition	授予检索列分区统计信息的权限	读取	database*		
			rootcatalog*		
			table*		
			catalog		
GetColumnStatisticsForTable	授予检索列的表统计信息的权限	读取	database*		
			rootcatalog*		
			table*		
			catalog		
GetColumnStatisticsTaskRun	授予根据运行 ID 检索表的列统计运行信息的权限	读取			
GetColumnStatisticsTaskRuns	授予根据运行 ID 检索表的列统计运行信息的权限	读取			
GetColumnStatisticsTaskSettings	授予检索列统计任务设置的权限	读取			
GetCompletion	授予从 Amazon Q 获取在 Glue 中为完成请求生成响应的权限	读取	completion*		
GetConnection	授予权限以检索连接	Read	connection*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			rootcatalog*		
GetConnections	授予权限以检索连接列表	Read	connection*		
			rootcatalog*		
GetCrawler	授予权限以检索爬网程序	Read	crawler*		
GetCrawlerMetrics	授予权限以检索有关爬网程序的指标	Read			
GetCrawlers	授予权限以检索所有爬网程序	读取			
GetCustomEntityType	授予权限以读取自定义实体类型	读取			
GetDashboardUrl	授予生成用于访问 spark live 用户界面的预签名网址的权限	读取	session*		
GetDataCatalogEncryptionSettings	授予权限以检索目录加密设置	读取	rootcatalog*		
GetDataPreviewStatement	授予权限以获取数据预览语句	权限管理			
GetDataQualityModel	授予权限以检索统计数据的预测模型的训练状态	读取	dataQualityRuleset*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			job*		
GetDataQualityModelResult	授予权限以从最新模型中检索统计数据的预测	读取	dataQualityRuleset*		
			job*		
GetDataQualityResult	授予权限以检索数据质量结果	读取	dataQualityRuleset*		
GetDataQualityRuleRecommendationRun	授予权限以检索数据质量规则建议运行	读取	dataQualityRuleset*		
GetDataQualityRuleset	授予权限以检索数据质量规则集	读取	dataQualityRuleset*		
GetDataQualityRulesetEvaluationRun	授予权限以检索数据质量规则建议运行	读取	dataQualityRuleset*		
GetDatabase	授予权限以检索数据库	Read	database*		
			rootcatalog*		
			catalog		
GetDatabases	授予权限以检索所有数据库	Read	database*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			rootcatalog*		
			catalog		
GetDataflowGraph	授予权限以将脚本转换为有向无环图 (DAG)	Read			
GetDevEndpoint	授予权限以检索开发终端节点	Read	devendpoint*		
GetDevEndpoints	授予权限以检索所有开发终端节点	读取			
GetEntityRecords	授予在胶水中预览实体记录的权限	读取	catalog*		
			connection		
GetEnvironment	授予权限以获取 SparkUI 的环境详细信息	权限管理			
GetExecutors	授予权限以获取 SparkUI 的执行程序	权限管理			
GetExecutorsThreads	授予权限以获取 SparkUI 的执行程序线程	权限管理			
GetGeneratedCode	将有向无环图 (DAG) 转换为代码	读取			
GetIntegrationResourceProperty	授予检索集成资源属性的权限	读取	catalog*		
			connection*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			database*		
GetIntegrationTableProperties	授予检索集成表属性的权限	读取	catalog*		
			connection*		
			database*		
GetJob	授予权限以检索作业	Read	job*		
GetJobBookmark	授予权限以检索作业书签	Read			
GetJobRun	授予权限以检索作业运行	Read	job*		
GetJobRuns	授予权限以检索作业的所有作业运行	读取	job*		
GetJobUpgradeAnalysis	授予检索任务升级分析的权限	读取	job*		
GetJobs	授予权限以检索所有当前作业	读取			
GetLogParsingStatus	授予权限以获取 SparkUI 的日志解析状态	权限管理			
GetMLTaskRun	授予权限以检索 ML 任务运行	Read	mlTransform*		
GetMLTaskRuns	授予权限以检索所有 ML 任务运行	List	mlTransform*		
GetMLTransform	授予权限以检索 ML 转换	Read	mlTransform*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetMLTransforms	授予权限以检索所有 ML 转换	List	mlTransform*		
GetMapping	授予权限以创建映射	读取			
GetNotebookInstanceStatus	授予权限以检索 Glue Studio 笔记本会话状态	权限管理			
GetPartition	授予权限以检索分区	读取	database*		
			rootcatalog*		
			table*		
			catalog		
GetPartitionIndexes	授予检索表的分区索引的权限	读取	database*		
			rootcatalog*		
			table*		
			catalog		
GetPartitions	授予权限以检索表的分区	Read	database*		
			rootcatalog*		
			table*		
			catalog		
GetPlan	授予权限以检索脚本映射	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetQueries	授予权限以获取 SparkUI 的查询	权限管理			
GetQuery	授予权限以获取 SparkUI 的特定查询	权限管理			
GetRecipeAction	授予权限以获取数据准备配方语句的结果	权限管理			
GetRegistry	授予检索架构注册表的权限	Read	registry*		
GetResourcePolicies	授予检索资源策略的权限	Read	rootcatalog*		
GetResourcePolicy	授予权限以检索资源策略	Read	rootcatalog*		
GetSchema	授予检索架构容器的权限	Read	registry*		
			schema*		
GetSchemaByDefinition	授予基于架构定义检索架构版本的权限	Read	registry*		
			schema*		
GetSchemaVersion	授予检索架构版本的权限	Read	registry		
			schema		
GetSchemaVersionsDiff	授予对比架构注册表中两个架构版本的权限	Read	registry*		
			schema*		
GetSecurityConfiguration	授予权限以检索安全配置	Read			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetSecurityConfigurations	授予权限以检索一个或多个安全配置	读取			
GetSession	授予检索交互式会话的权限	读取	session*		
GetStage	授予权限以获取 SparkUI 的阶段	权限管理			
GetStageAttempt	授予权限以获取 SparkUI 的阶段尝试	权限管理			
GetStageAttemptTaskList	授予权限以获取 SparkUI 的阶段尝试任务列表	权限管理			
GetStageAttemptTaskSummary	授予权限以获取 SparkUI 的阶段尝试任务摘要	权限管理			
GetStageFiles	授予权限以获取 SparkUI 的阶段文件	权限管理			
GetStages	授予权限以获取 SparkUI 的阶段	权限管理			
GetStatement	授予权限以检索交互式会话中语句的相关结果和信息	读取	session*		
GetStorage	授予权限以获取 SparkUI 的存储详细信息	权限管理			
GetStorageUnit	授予权限以获取 SparkUI 的存储单位详细信息	权限管理			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetTable	授予权限以检索表	读取	database*		
			rootcatalog*		
			table*		
			catalog		
GetTableOptimizer	授予返回与指定表关联的所有优化器的配置的权限	读取	database*		glue:GetTable
			rootcatalog*		
			table*		
GetTableVersion	授予权限以检索表版本	Read	database*		
			rootcatalog*		
			table*		
			catalog		
GetTableVersions	授予权限以检索表版本列表	Read	database*		
			rootcatalog*		
			table*		
			catalog		
GetTables	授予权限以检索数据库中的表	Read	database*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			rootcatalog*		
			table*		
			catalog		
GetTags	授予权限以检索与资源关联的所有标签	Read	blueprint		
			crawler		
			customEntityType		
			devendpoint		
			job		
			trigger		
			usageProfile		
			workflow		
GetTrigger	授予权限以检索触发器	Read	trigger*		
GetTriggers	授予权限以检索与作业关联的触发器	读取			
GetUsageProfile	授予权限以检索使用情况配置文件	读取	usageProfile*		
GetUserDefinedFunction	授予权限以检索函数定义	读取	database*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			rootcatalog*		
			userdefinedfunction*		
			catalog		
GetUserDefinedFunctions	授予权限以检索多个函数定义	Read	database*		
			rootcatalog*		
			userdefinedfunction*		
			catalog		
GetWorkflow	授予权限以检索工作流程	Read	workflow*		
GetWorkflowRun	授予权限以检索工作流程运行	Read	workflow*		
GetWorkflowRunProperties	授予权限以检索工作流程运行属性	Read	workflow*		
GetWorkflowRuns	授予权限以检索工作流程的所有运行	读取	workflow*		
GlueNotebookAuthorize	授予权限以访问 Glue Studio 笔记本	权限管理			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GlueNotebookRefreshCredentials	授予权限以刷新 Glue Studio 笔记本凭证	权限管理			
ImportCatalogToGlue	授予将 Athena 数据目录导入 Glue 的权限 Amazon	写入	rootcatalog*		
ListBlueprints	授予权限以检索所有蓝图	列表			
ListColumnStatisticsTaskRuns	授予列出已为账户执行的所有列统计信息运行 ID 的权限	读取			
ListConnectionTypes	授予权限以在 Glue Studio 中列出连接类型	权限管理			
ListCrawlers	授予权限以检索所有爬网程序	列表			
ListCrawls	授予权限以检索爬网程序的爬取运行历史	列表	crawler*		
ListCustomEntityTypes	授予权限以检索所有自定义实体类型	列表			
ListDataQualityResults	授予权限以检索所有数据质量结果	列表	dataQualityRuleset*		
ListDataQualityRuleRecommendationRuns	授予权限以检索所有数据质量规则建议运行	列表	dataQualityRuleset*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListDataQualityRulesetEvaluationRuns	授予权限以检索所有数据质量规则建议运行	列表	dataQualityRuleset*		
ListDataQualityRulesets	授予权限以检索数据质量规则集列表	列表	dataQualityRuleset*		
ListDevEndpoints	授予权限以检索所有开发终端节点	列表			
ListEntities	授予权限以在 Glue Studio 中列出实体	权限管理	connection*		
			rootcatalog*		
ListJobUpgradeAnalyses	授予列出任务升级分析的权限	列表	job*		
ListJobs	授予权限以检索所有当前作业	List			
ListMLTransforms	授予权限以检索所有 ML 转换	List	mlTransform*		
ListRegistries	授予检索架构注册表列表的权限	List			
ListSchemaVersions	授予检索架构版本列表的权限	List	registry*		
			schema*		
ListSchemas	授予检索架构容器列表的权限	列表	registry		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListSessions	授予检索交互式会话列表的权限	列表			
ListStatements	授予检索交互式会话中语句列表的权限	列表	session*		
ListTableOptimizerRuns	授予列出特定表的以前优化器运行的历史记录的权限	列表	database*		glue:GetTable
			rootcatalog*		
			table*		
ListTriggers	授予权限以检索所有触发器	列表			
ListUsageProfiles	授予权限以检索使用情况配置文件列表	列表			
ListWorkflows	授予权限以检索所有工作流程	列表			
ModifyIntegration	授予修改零 ETL 集成的权限	写入	integration*		
				aws:ResourceTag/${TagKey}	
NotifyEvent	授予向事件驱动工作流通知事件的权限	写入	workflow*		
PassConnection[仅权限]	授予在输入中传递需要粘合连接名称 APIs 的权限	写入	connection*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PublishDataQuality[仅权限]	授予权限以发布数据质量结果	写入	dataQualityRuleset*		
PutDataCatalogEncryptionSettings	授予权限以更新目录加密设置	写入	rootcatalog*		
PutDataQualityProfileAnnotation	授予权限以对配置文件的所有数据点进行注释	写入	dataQualityRuleset*		
			job*		
PutDataQualityStatisticAnnotation	授予权限以对特定数据质量统计数据随时间变化的数据点进行注释	写入	dataQualityRuleset*		
			job*		
PutResourcePolicy	授予权限以更新资源策略	Permissions management	rootcatalog*		
PutSchemaVersionMetadata	授予向架构版本添加元数据的权限	Write	registry		
			schema		
PutWorkflowRunProperties	授予权限以更新工作流程运行属性	Write	workflow*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
QuerySchemaVersionMetadata	授予获取架构版本元数据的权限	列表	registry		
			schema		
RefreshOAuth2Tokens	授予权限以在任务执行期间刷新 oauth2 令牌以进行连接	权限管理	connection*		
			rootcatalog*		
RegisterSchemaVersion	授予创建新架构版本的权限	Write	registry*		
			schema*		
RemoveSchemaVersionMetadata	授予从架构版本中删除元数据的权限	写入	registry		
			schema		
RequestLogParsing	授予权限以请求 SparkUI 的日志解析	权限管理			
ResetJobBookmark	授予权限以重置作业书签	Write			
ResumeWorkflowRun	授予权限以恢复工作流程运行	写入	workflow*		
RunDataPreviewStatement	授予权限以运行数据预览语句	权限管理			
RunStatement	授予权限以运行交互式会话中的代码或语句	写入	session*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
SearchTables	授予权限以检索目录中的表	读取	database*		
			rootcatalog*		
			table*		
			catalog		
SendFeedback	授予在 Amazon Q 中提供有关 glue 完成体验的反馈的权限	写入			
SendRecipeAction	授予权限以在数据预览中执行数据准备配方语句	权限管理			
StartBlueprintRun	授予权限以开始运行蓝图	写入	blueprint*		
StartColumnStatisticsTaskRun	授予启动运行以生成表的列统计信息的权限	写入	database*		glue:GetSecurityConfiguration glue:GetTable
			rootcatalog*		
			table*		
StartColumnStatisticsTaskRunSchedule	授予启动列统计任务运行计划的权限	写入	database*		
			rootcatalog*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			table*		
StartCompletion	授予在 Glue for Amazon Q 体验中创建完成请求的权限	写入			
StartCrawler	授予权限以启动爬网程序	Write	crawler*		
StartCrawlerSchedule	授予权限以将爬网程序的计划状态更改为 SCHEDULED	写入			
StartDataQualityRuleRecommendationRun	授予权限以开始数据质量规则建议运行	写入	dataQualityRuleset*		
StartDataQualityRulesetEvaluationRun	授予权限以开始数据质量规则建议运行	写入	dataQualityRuleset*		
StartExportLabelsTaskRun	授予权限以启动导出标签 ML 任务运行	Write	mlTransform*		
StartImportLabelsTaskRun	授予权限以启动导入标签 ML 任务运行	Write	mlTransform*		
StartJobRun	授予权限以开始运行作业	写入	job*		
StartJobUpgradeAnalysis	授予开始为作业运行升级分析的权限	写入	job*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StartMLEvaluationTaskRun	授予权限以启动评估 ML 任务运行	Write	mlTransform*		
StartMLLabelingSetGenerationTaskRun	授予权限以启动标签集生成 ML 任务运行	写入	mlTransform*		
StartNotebook	授予权限以开始 Glue Studio 笔记本	权限管理			
StartTrigger	授予权限以启动触发器	Write	trigger*		
StartWorkflowRun	授予权限以开始运行工作流程	写入	workflow*		
StopColumnStatisticsTaskRun	授予停止列统计信息运行的执行的权限	写入	database*		
			rootcatalog*		
			table*		
StopColumnStatisticsTaskRunSchedule	授予停止列统计任务运行计划的权限	写入	database*		
			rootcatalog*		
			table*		
StopCrawler	授予权限以停止运行的爬网程序	Write	crawler*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StopCrawlerSchedule	授予权限以将爬网程序的计划状态设置为 NOT_SCHEDULED	写入			
StopJobUpgradeAnalysis	授予停止正在进行的任务升级分析的权限	写入	job*		
StopSession	授予停止交互式会话的权限	写入	session*		
StopTrigger	授予权限以停止触发器	Write	trigger*		
StopWorkflowRun	授予权限以停止工作流程运行	Write	workflow*		
TagResource	授予权限以将标签添加到资源中	标记	blueprint		
			connection		
			crawler		
			customEntityType		
			dataQualityRuleset		
			devendpoint		
			integration		
			job		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			mlTransform		
			registry		
			schema		
			session		
			trigger		
			usageProfile		
			workflow		
				aws:TagKeys aws:RequestTag/${TagKey}	
TerminateNotebook	授予权限以终止 Glue Studio 笔记本	权限管理			
TestConnection	授予在 Glue Studio 中测试连接的权限	权限管理			
UntagResource	授予权限以删除与资源关联的标签	标记	blueprint		
			connection		
			crawler		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			customEntityType		
			dataQualityRuleset		
			devendpoint		
			integration		
			job		
			mlTransform		
			registry		
			schema		
			session		
			trigger		
			usageProfile		
			workflow		
				aws:TagKeys	
UpdateBlueprint	授予权限以更新蓝图	写入	blueprint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateCatalog	授予更新目录的权限	写入	rootcatalog*		
			catalog		
UpdateClassifier	授予权限以更新分类器	写入			
UpdateColumnStatisticsForPartition	授予更新列分区统计信息的权限	写入	database*		
			rootcatalog*		
			table*		
			catalog		
UpdateColumnStatisticsForTable	授予更新列的表统计信息的权限	写入	database*		
			rootcatalog*		
			table*		
			catalog		
UpdateColumnStatisticsTaskSettings	授予更新列统计任务设置的权限	写入	database*		
			rootcatalog*		
			table*		
UpdateConnection	授予权限以更新连接	Write	connection*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			rootcatalog*		
UpdateCrawler	授予权限以更新爬网程序	Write	crawler*		
UpdateCrawlerSchedule	授予权限以更新爬网程序的计划	写入			
UpdateDataQualityRuleset	授予权限以更新数据质量规则集	写入	dataQualityRuleset*		
UpdateDatabase	授予权限以更新数据库	Write	database*		
			rootcatalog*		
			catalog		
UpdateDevEndpoint	授予权限以更新开发终端节点	写入	devendpoint*		
UpdateIntegrationResourceProperty	授予更新集成资源属性的权限	写入	catalog*		
			connection*		
			database*		
UpdateIntegrationTableProperties	授予更新集成表属性的权限	写入	catalog*		
			connection*		
			database*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateJob	授予权限以更新作业	写入	job*		
				glue:VpcIds glue:SubnetIds glue:SecurityGroupIds	
UpdateJobFromSourceControl	授予从来源控制提供程序更新作业的权限	写入	job*		
UpdateMLTransform	授予权限以更新 ML 转换	Write	mlTransform*		
UpdatePartition	授予权限以更新分区	Write	database*		
			rootcatalog*		
			table*		
			catalog		
UpdateRegistry	授予更新架构注册表的权限	Write	registry*		
UpdateSchema	授予更新架构容器的权限	写入	registry*		
			schema*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateSourceControlFromJob	授予从作业更新来源控制提供程序的权限	写入	job*		
UpdateTable	授予权限以更新表	写入	database*		
			rootcatalog*		
			table*		
			catalog		
UpdateTableOptimizer	授予更新现有表优化器的配置的权限	写入	database*		glue:GetTable
			rootcatalog*		
			table*		
UpdateTrigger	授予权限以更新触发器	写入	trigger*		
UpdateUsageProfile	授予权限以更新配置文件	写入	usageProfile*		
UpdateUserDefinedFunction	授予权限以更新函数定义	Write	database*		
			rootcatalog*		
			userdefinedfunction*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			catalog		
UpdateWorkflow	授予权限以更新工作流程	写入	workflow*		
UpgradeJob	授予将任务升级到最新版本的权限	写入	job*		
UseGlueStudio	授予使用 Glue Studio 和访问其内部内容的权限 APIs	权限管理			
UseMLTransforms[仅权限]	授予权限以从 Glue ETL 脚本中使用 ML 转换	Write	mlTransform*		

Amazon Glue 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
rootcatalog	`arn:${Partition}:glue:${Region}:${Account}:catalog`	
catalog	`arn:${Partition}:glue:${Region}:${Account}:catalog/${CatalogName}`	
database	`arn:${Partition}:glue:${Region}:${Account}:database/${DatabaseName}`	

资源类型	ARN	条件键
table	arn:${Partition}:glue:${Region}:${Account}:table/${DatabaseName}/${TableName}	
tableversion	arn:${Partition}:glue:${Region}:${Account}:tableVersion/${DatabaseName}/${TableName}/${TableVersionName}	
connection	arn:${Partition}:glue:${Region}:${Account}:connection/${ConnectionName}	aws:ResourceTag/${TagKey}
userdefinedfunction	arn:${Partition}:glue:${Region}:${Account}:userDefinedFunction/${DatabaseName}/${UserDefinedFunctionName}	
devendpoint	arn:${Partition}:glue:${Region}:${Account}:devEndpoint/${DevEndpointName}	aws:ResourceTag/${TagKey}
job	arn:${Partition}:glue:${Region}:${Account}:job/${JobName}	aws:ResourceTag/${TagKey}
trigger	arn:${Partition}:glue:${Region}:${Account}:trigger/${TriggerName}	aws:ResourceTag/${TagKey}
crawler	arn:${Partition}:glue:${Region}:${Account}:crawler/${CrawlerName}	aws:ResourceTag/${TagKey}
workflow	arn:${Partition}:glue:${Region}:${Account}:workflow/${WorkflowName}	aws:ResourceTag/${TagKey}
blueprint	arn:${Partition}:glue:${Region}:${Account}:blueprint/${BlueprintName}	aws:ResourceTag/${TagKey}
mlTransform	arn:${Partition}:glue:${Region}:${Account}:mlTransform/${TransformId}	aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
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}

Amazon Glue 的条件键

Amazon Glue 定义了以下可在 IAM 策略Condition元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对来筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按附加到资源的标签键值对筛选操作	字符串
aws:TagKeys	根据在请求中是否具有标签键来筛选访问	ArrayOfString
glue:CredentialIssuingService	按发出请求凭据的服务筛选访问权限	字符串
glue:EnabledForRedshiftAutoDiscovery	根据是否存在为角色的基于身份的策略配置的密钥来筛选访问权限	布尔型
glue:RoleAssumedBy	通过担任客户角色从中获取请求凭据的服务筛选访问权限	字符串
glue:SecurityGroupIds	按为 Glue 作业配置的安全组的 ID 筛选访问	ArrayOfString
glue:SubnetIds	根据为 Glue 作业配置的子网 ID 过滤访问	ArrayOfString
glue:VpcIds	根据为 Glue 作业配置的 VPC ID 过滤访问	ArrayOfString

Glue 的操作、资源和条件 Amazon 键 DataBrew

Amazon Glue DataBrew （服务前缀:`databrew`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。

- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Glue 定义的动作 DataBrew
- 由 Amazon Glue 定义的资源类型 DataBrew
- Amazon Glue 的条件键 DataBrew

Amazon Glue 定义的动作 DataBrew

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchDeleteRecipeVersion	授予删除一个或多个配方版本的权限	Write	Recipe*		
CreateDataset	授予创建数据集的权限	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfileJob	授予创建配置文件作业的权限	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProject	授予权限以创建项目	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRecipe	授予创建配方的权限	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRecipeJob	授予创建配方作业的权限	写入		aws:RequestTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys	
CreateRuleset	授予权限以创建规则集	写入		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSchedule	授予创建计划的权限	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDataset	授予删除数据库的权限	Write	Dataset*		
DeleteJob	授予权限以删除作业	Write	Job*		
DeleteProject	授予权限以删除项目	Write	Project*		
DeleteRecipeVersion	授予删除配方版本的权限	写入	Recipe*		
DeleteRuleset	授予删除规则集的权限	写入	Ruleset*		
DeleteSchedule	授予删除计划的权限	Write	Schedule*		
DescribeDataset	授予查看有关数据集详细信息的权限	Read	Dataset*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeJob	授予查看有关作业详细信息的权限	Read	Job*		
DescribeJobRun	授予权限以查看给定作业的作业运行详细信息	Read	Job*		
DescribeProject	授予查看有关项目详细信息的权限	Read	Project*		
DescribeRecipe	授予查看有关配方详细信息的权限	读取	Recipe*		
DescribeRuleset	授予查看有关规则集详细信息的权限	读取	Ruleset*		
DescribeSchedule	授予查看有关计划详细信息的权限	Read	Schedule*		
ListDatasets	授予列出账户中的数据集的权限	Read			
ListJobRuns	授予列出给定作业的作业运行的权限	Read	Job*		
ListJobs	授予列出账户中的作业的权限	Read			
ListProjects	授予列出账户中的项目的权限	Read			
ListRecipeVersions	授予列出配方中的版本的权限	Read	Recipe*		
ListRecipes	授予列出账户中的配方的权限	读取			
ListRulesets	授予列出账户中的规则集的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListSchedules	授予列出账户中的计划的权限	Read			
ListTagsForResource	授予检索与资源关联的标签的权限	Read	Dataset		
			Job		
			Project		
			Recipe		
			Ruleset		
			Schedule		
PublishRecipe	授予发布配方主版本的权限	Write	Recipe*		
SendProjectSessionAction	授予向项目的交互式会话提交操作的权限	Write	Project*		
StartJobRun	授予权限以开始运行作业	Write	Job*		
StartProjectSession	授予启动项目交互式会话的权限	Write	Project*		
StopJobRun	授予停止作业运行的权限	Write	Job*		
TagResource	授予权限以将标签添加到资源中	Tagging	Dataset		
			Job		
			Project		
			Recipe		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			Ruleset		
			Schedule		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予权限以删除与资源关联的标签	Tagging	Dataset		
			Job		
			Project		
			Recipe		
			Ruleset		
			Schedule		
				aws:TagKeys	
UpdateDataset	授予修改数据集的权限	Write	Dataset*		
UpdateProfileJob	授予修改配置文件作业的权限	Write	Job*		
UpdateProject	授予修改项目的权限	Write	Project*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateRecipe	授予修改配方的权限	Write	Recipe*		
UpdateRecipeJob	授予修改配方作业的权限	写入	Job*		
UpdateRuleset	授予修改规则集的权限	写入	Ruleset*		
UpdateSchedule	授予修改计划的权限	写入	Schedule*		

由 Amazon Glue 定义的资源类型 DataBrew

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
Project	`arn:${Partition}:databrew:${Region}:${Account}:project/${ResourceId}`	aws:ResourceTag/${TagKey}
Dataset	`arn:${Partition}:databrew:${Region}:${Account}:dataset/${ResourceId}`	aws:ResourceTag/${TagKey}
Ruleset	`arn:${Partition}:databrew:${Region}:${Account}:ruleset/${ResourceId}`	aws:ResourceTag/${TagKey}
Recipe	`arn:${Partition}:databrew:${Region}:${Account}:recipe/${ResourceId}`	aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
Job	arn:${Partition}:databrew:${Region}:${Account}:job/${ResourceId}	aws:ResourceTag/${TagKey}
Schedule	arn:${Partition}:databrew:${Region}:${Account}:schedule/${ResourceId}	aws:ResourceTag/${TagKey}

Amazon Glue 的条件键 DataBrew

Amazon Glu DataBrew e 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString

Amazon 的操作、资源和条件密钥 GuardDuty

Amazon GuardDuty （服务前缀:guardduty）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon 定义的操作 GuardDuty

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AcceptAdministratorInvitation	授予接受成为 GuardDuty 成员账户的邀请的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AcceptInvitation	授予接受成为 GuardDuty 成员账户的邀请的权限	写入			
ArchiveFindings	授予存档 GuardDuty 调查结果的权限	写入			
CreateDetector	授予权限以创建检测器	写入		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFilter	授予创建 GuardDuty 过滤器的权限。筛选条件定义用于筛选结果的结果属性和条件	写入	filter*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIPSet	授予创建 IPSet	写入		aws:RequestTag/${TagKey} aws:TagKeys	iam:DeleteRolePolicy iam:PutRolePolicy
CreateMalwareProtectionPlan	授予权限以创建新恶意软件防护计划	写入		aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateMembers	授予创建 GuardDuty 成员账户的权限，其中用于创建成员的账户变为 GuardDuty 管理员账户	写入			
CreatePublishingDestination	授予权限以创建发布目标	Write			s3:GetObject s3:ListBucket
CreateSampleFindings	授予权限以创建示例结果	写入			
CreateThreatIntelSet	授予创建权限 GuardDuty ThreatIntelSets，其中 ThreatIntelSet 包含用于生成发现结果的已知恶意 IP 地址 GuardDuty	写入		aws:RequestTag/${TagKey} aws:TagKeys	
DeclineInvitations	授予拒绝邀请成为 GuardDuty 成员账户的权限	写入			
DeleteDetector	授予删除探 GuardDuty 测器的权限	写入	detector*		
DeleteFilter	授予删除 GuardDuty 过滤器的权限	写入	filter*		
DeleteIPSet	授予删除权限 GuardDuty IPSets	写入	ipset*		
DeleteInvitations	授予删除成为 GuardDuty 成员账户的邀请的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteMalwareProtectionPlan	授予权限以删除恶意软件防护计划	写入	malwareprotectionplan*		
DeleteMembers	授予删除 GuardDuty 成员账户的权限	写入			
DeletePublishingDestination	授予权限以删除发布目标	写入	publishingDestination*		
DeleteThreatIntelSet	授予删除权限 GuardDuty ThreatIntelSets	写入	threatintelset*		
DescribeMalwareScans	授予权限以检索有关恶意软件扫描的详细信息	读取			
DescribeOrganizationConfiguration	授予权限以检索与 GuardDuty 探测器关联的委派管理员的详细信息	读取			
DescribePublishingDestination	授予权限以检索有关发布目标的详细信息	读取	publishingDestination*		
DisableOrganizationAdminAccount	授予禁用组织委托管理员的权限 GuardDuty	写入			
DisassociateFromAdministratorAccount	授予取消 GuardDuty 成员账户与其 GuardDuty 管理员账户关联的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DisassociateFromMasterAccount	授予取消 GuardDuty 成员账户与其 GuardDuty 管理员账户关联的权限	写入			
DisassociateMembers	授予取消 GuardDuty 成员账户与其管理员 GuardDuty 账户关联的权限	写入			
EnableOrganizationAdminAccount	授予允许组织委托管理员执行以下操作的权限 GuardDuty	写入			
GetAdministratorAccount	授予检索与成员账户关联的 GuardDuty 管理员账户详细信息的权限	读取			
GetCoverageStatistics	授予列出某地区指定 GuardDuty 账户的 Amazon GuardDuty 覆盖率统计数据的权限	读取	detector*		
GetDetector	授予检索 GuardDuty 探测器的权限	读取	detector*		
GetFilter	授予检索 GuardDuty 过滤器的权限	读取	filter*		
GetFindings	授予检索 GuardDuty 结果的权限	读取			
GetFindingsStatistics	授予检索 GuardDuty 查找结果统计信息列表的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetIPSet	授予检索权限 GuardDuty IPSets	读取	ipset*		
GetInvitationsCount	授予权限以检索发送到指定账户的所有 GuardDuty 邀请的数量，其中不包括已接受的邀请	读取			
GetMalwareProtectionPlan	授予权限以检索恶意软件防护计划详细信息	读取	malwareprotectionplan*		
GetMalwareScanSettings	授予权限以检索恶意软件扫描设置	读取			
GetMasterAccount	授予检索与成员账户关联的 GuardDuty 管理员账户详细信息的权限	读取			
GetMemberDetectors	授予权限以描述为成员账户检测器启用的数据源	读取			
GetMembers	授予权限以检索与管理员账户关联的成员账户	读取			
GetOrganizationStatistics	授予检索某地区成员账户的 GuardDuty 保护计划覆盖范围统计数据的权限	读取			
GetRemainingFreeTrialDays	授予提供免费试用期内使用的每个数据来源的剩余天数的权限	读取			
GetThreatIntelSet	授予检索权限 GuardDuty ThreatIntelSets	读取	threatintelset*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetUsageStatistics	允许列出指定探测器 ID 在过去 30 天内的 Amazon GuardDuty 使用统计数据	读取			
InviteMembers	授予邀请其他 Amazon 账户启用 GuardDuty 和成为 GuardDuty 成员账户的权限	写入			
ListCoverage	授予权限以列出某个区域内给定账户的所有资源详细信息	列表	detector*		
ListDetectors	授予检索 GuardDuty 探测器列表的权限	列表			
ListFilters	授予检索 GuardDuty 筛选器列表的权限	列表			
ListFindings	授予检索 GuardDuty 发现结果列表的权限	列表			
ListIPSets	授予检索列表的权限 GuardDuty IPSets	列表			
ListInvitations	授予权限以检索已发送给的所有 GuardDuty 成员资格邀请的列表 Amazon Web Services 账户	列表			
ListMalwareProtectionPlans	授予权限以检索恶意软件防护计划列表	列表			
ListMembers	授予检索与管理员账户关联的 GuardDuty 成员账户列表的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListOrganizationAdminAccounts	授予列出组织委托管理员详细信息的权限 GuardDuty	列表			
ListPublishingDestinations	授予权限以检索发布目标的列表	列表			
ListTagsForResource	授予检索与 GuardDuty 资源关联的标签列表的权限	读取	detector		
			filter		
			ipset		
			malwareprotectionplan		
			threatintelset		
ListThreatIntelSets	授予检索列表的权限 GuardDuty ThreatIntelSets	列表			
SendSecurityTelemetry	授予为区域内特定 GuardDuty 账户发送安全遥测数据的权限	写入			
StartMalwareScan	授予权限以发起新的恶意软件扫描	写入			
StartMonitoringMembers	向 GuardDuty 管理员账户授予权限以监控来自 GuardDuty 成员账户的调查结果	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StopMonitoringMembers	授予权限以禁用成员账户的监控结果	写入			
TagResource	授予向 GuardDuty 资源添加标签的权限	标记	detector		
			filter		
			ipset		
			malwareprotectionplan		
			threatintelset		
				aws:RequestTag/${TagKey} aws:TagKeys	
Unarchive Findings	授予取消存档结果的 GuardDuty 权限	写入			
UntagResource	授予从 GuardDuty 资源中移除标签的权限	标记	detector		
			filter		
			ipset		
			malwareprotectionplan		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			threatintelset		
				aws:TagKeys	
UpdateDetector	授予更新探 GuardDuty 测器的权限	写入	detector*		
UpdateFilter	授予更新 GuardDuty 过滤器的权限	写入	filter*		
UpdateFindingsFeedback	授予更新调查结果反馈以将 GuardDuty 结果标记为有用或无用的权限	写入			
UpdateIPSet	授予更新权限 GuardDuty IPSets	写入	ipset*		iam:DeleteRolePolicy iam:PutRolePolicy
UpdateMalwareProtectionPlan	授予权限以更新恶意软件防护计划	写入	malwareprotectionplan*		
UpdateMalwareScanSettings	授予权限以更新恶意软件扫描设置	写入			
UpdateMemberDetectors	授予权限以更新为成员账户检测器启用的数据源	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateOrganizationConfiguration	授予更新与 GuardDuty 探测器关联的委派管理员配置的权限	写入			
UpdatePublishingDestination	授予权限以更新发布目标	写入	publishingDestination*		s3:GetObject s3:ListBucket
UpdateThreatIntelSet	授予更新权限 GuardDuty ThreatIntelSets	写入	threatintelset*		iam:DeleteRolePolicy iam:PutRolePolicy

Amazon 定义的资源类型 GuardDuty

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
detector	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}`	aws:ResourceTag/${TagKey}
filter	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/filter/${FilterName}`	aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
ipset	arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/ipset/${IPSetId}	aws:ResourceTag/${TagKey}
threatintelset	arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/threatintelset/${ThreatIntelSetId}	aws:ResourceTag/${TagKey}
publishingDestination	arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/publishingDestination/${PublishingDestinationId}	
malwareprotectionplan	arn:${Partition}:guardduty:${Region}:${Account}:malware-protection-plan/${MalwareProtectionPlanId}	aws:ResourceTag/${TagKey}

Amazon 的条件密钥 GuardDuty

Amazon GuardDuty 定义了以下可在 IAM 策略Condition元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中的标签键值对筛选访问	字符串
aws:ResourceTag/${TagKey}	按附加到资源的标签键值对筛选操作	字符串
aws:TagKeys	按请求中的标签键筛选访问权限	ArrayOfString

Healt Amazon h 和 Notifications 的操作、资源 APIs 和条件键

Amazon Heal APIs th and Notifications（服务前缀:health）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

由 “Healt Amazon h” APIs 和 “通知” 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeAffectedAccountsForOrganization	授予检索组织中受指定事件影响的账户列表的权限	读取			organizations:ListAccounts
DescribeAffectedEntities	授予检索受指定事件影响的实体列表的权限	读取	event*		
				health:eventTypeCode health:service	
DescribeAffectedEntitiesForOrganization	授予检索组织中受指定事件和账户影响的实体列表的权限	读取			organizations:ListAccounts
DescribeEntityAggregates	授予检索受每种指定事件影响的实体数量的权限	读取			
DescribeEntityAggregatesForOrganization	授予检索受组织中的每种指定事件影响的实体数量的权限	读取			organizations:ListAccounts
DescribeEventAggregates	授予检索每种事件类型（问题、计划的更改和账户通知）的事件数的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeEventDetails	授予检索与一个或多个指定事件相关的详细信息的权限	读取	event*		
				health:eventTypeCode health:service	
DescribeEventDetailsForOrganization	授予检索与组织中提供账户的一个或多个指定事件相关的详细信息的权限	读取			organizations:ListAccounts
DescribeEventTypes	授予检索符合指定筛选条件的事件类型的权限	读取			
DescribeEvents	授予检索与符合指定筛选条件的事件相关的信息的权限	读取			
DescribeEventsForOrganization	授予检索与符合组织的指定筛选条件的事件相关的信息的权限	读取			organizations:ListAccounts
DescribeHealthServiceStatusForOrganization	授予检索启用或禁用组织视图功能的状态的权限	读取			organizations:ListAccounts

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DisableHealthServiceAccessForOrganization	授予禁用组织视图功能的权限	权限管理			organizations:DisableAWSServiceAccess organizations:ListAccounts
EnableHealthServiceAccessForOrganization	授予启用组织视图功能的权限	权限管理			iam:CreateServiceLinkedRole organizations:EnableAWSServiceAccess organizations:ListAccounts

由 “Healt Amazon h” APIs 和 “通知” 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
event	arn:${Partition}:health:*::event/${Service}/${EventTypeCode}/*	

Healt Amazon h APIs 和通知的条件键

Amazon Heal APIs th and Notifications 定义了以下可用于 IAM 策略Condition元素的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
health:eventTypeCode	按事件类型筛选访问权限	字符串
health:service	按受影响的服务筛选访问权限	字符串

Amazon IAM Access Analyzer 的操作、资源和条件键

Amazon IAM Access Analyzer（服务前缀:access-analyzer）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon IAM Access Analyzer 定义的操作
- Amazon IAM Access Analyzer 定义的资源类型
- Amazon IAM Access Analyzer 的条件键

Amazon IAM Access Analyzer 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ApplyArchiveRule	授予应用存档规则的权限	Write	Analyzer*		
CancelPolicyGeneration	授予取消策略生成的权限	写入			
CheckAccessNotGranted	授予检查策略是否不允许指定访问的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CheckNoNewAccess	授予检查现有策略是否不允许新访问权限的权限	读取			
CheckNoPublicAccess	授予权限以检查资源策略是否不允许公共访问	读取			
CreateAccessPreview	授予权限以为指定分析器创建访问预览	Write	Analyzer*		
CreateAnalyzer	授予权限以创建分析器	Write	Analyzer*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateArchiveRule	授予权限以为指定分析器创建存档规则	Write	ArchiveRule*		
DeleteAnalyzer	授予权限以删除指定的分析器	Write	Analyzer*		
DeleteArchiveRule	授予权限以删除指定分析器的存档规则	写入	ArchiveRule*		
GenerateFindingRecommendation	授予权限以生成用于解析调查发现的建议步骤	写入	Analyzer*		
GetAccessPreview	授予权限以检索有关访问预览的信息	Read	Analyzer*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetAnalyzedResource	授予权限以检索有关已分析资源的信息	Read	Analyzer*		
GetAnalyzer	授予权限以检索有关分析器的信息	Read	Analyzer*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetArchiveRule	授予权限以检索有关指定分析器的存档规则的信息	Read	ArchiveRule*		
GetFinding	授予权限以检索结果	读取	Analyzer*		
GetFindingRecommendation	授予权限以检索用于解析调查发现的建议步骤	读取	Analyzer*		
GetFindingsStatistics	授予检索调查发现统计数据的权限	读取	Analyzer*		
GetGeneratedPolicy	授予权限以检索使用生成的策略 StartPolicyGeneration	读取			
ListAccessPreviewFindings	授予权限以从访问预览中检索结果的列表	Read	Analyzer*		
ListAccessPreviews	授予权限以检索访问预览的列表	List	Analyzer*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListAnalyzedResources	授予权限以检索已分析资源的列表	Read	Analyzer*		
ListAnalyzers	授予权限以检索分析器列表	List			
ListArchiveRules	授予权限以从分析器中检索存档规则的列表	List	Analyzer*		
ListFindings	授予权限以从分析器中检索结果的列表	Read	Analyzer*		
ListPolicyGenerations	授予权限以列出所有最近启动的策略生成	Read			
ListTagsForResource	授予权限以检索应用于资源的标签的列表	Read	Analyzer		
StartPolicyGeneration	授予权限以启动策略生成	Write			iam:PassRole
StartResourceScan	授予权限以开始扫描应用于资源的策略	Write	Analyzer*		
TagResource	授予权限以将标签添加到资源	Tagging	Analyzer		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予权限以从资源中删除标签	标记	Analyzer		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys	
UpdateAnalyzer	授予修改分析器配置的权限	写入	Analyzer*		
UpdateArchiveRule	授予权限以修改存档规则	Write	ArchiveRule*		
UpdateFindings	授予权限以修改结果	Write	Analyzer*		
ValidatePolicy	授予验证策略的权限	Read			

Amazon IAM Access Analyzer 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
Analyzer	`arn:${Partition}:access-analyzer:${Region}:${Account}:analyzer/${AnalyzerName}`	aws:ResourceTag/${TagKey}
ArchiveRule	`arn:${Partition}:access-analyzer:${Region}:${Account}:analyzer/${AnalyzerName}/archive-rule/${RuleName}`	

Amazon IAM Access Analyzer 的条件键

Amazon IAM Access Analyzer 定义了以下可以在 IAM 策略Condition元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对以筛选操作	字符串
aws:ResourceTag/${TagKey}	根据附加到资源的标签键值对筛选操作	字符串
aws:TagKeys	根据在请求中是否具有标签键以筛选操作	ArrayOfString

Amazon IAM 身份中心（ Amazon 单点登录的继任者）的操作、资源和条件密钥

Amazon IAM Identity Center（ Amazon 单点登录的继任者sso）（服务前缀:）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- 由 Amazon IAM 身份中心（ Amazon 单点登录的继任者）定义的操作
- 由 Amazon IAM 身份中心（ Amazon 单点登录的继任者）定义的资源类型
- Amazon IAM 身份中心（ Amazon 单点登录的继任者）的条件密钥

由 Amazon IAM 身份中心（ Amazon 单点登录的继任者）定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateDirectory	授予连接 Amazon IAM 身份中心使用的目录的权限	写入			ds:AuthorizeApplication
AssociateProfile	授予权限以在目录用户或组与配置文件之间创建关联	写入			
AttachCustomerManagedPolicy	授予权限以将客户管理型策略参考附加到权限集	权限管理	Instance*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ReferenceToPermissionSet			PermissionSet*		
AttachManagedPolicyToPermissionSet	授予将 Amazon 托管策略附加到权限集的权限	权限管理	Instance*		
			PermissionSet*		
CreateAccountAssignment	授予 Amazon Web Services 账户 使用指定权限集向指定委托人分配访问权限的权限	写入	Account*		
			Instance*		
			PermissionSet*		
CreateApplication	授予创建应用程序的权限	写入	ApplicationProvider*		
			Instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateApplicationAssignment	授予创建应用程序分配的权限	写入	Application*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				sso:ApplicationAccount	
CreateApplicationInstance	授予向 Amazon IAM 身份中心添加应用程序实例的权限	写入			
CreateApplicationInstanceCertificate	授予权限以为应用程序实例添加新证书	写入			
CreateInstance	授予创建 Identity Center 实例的权限	写入	Instance*		iam:CreateServiceLinkedRole organizations:DescribeOrganization
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateInstanceAccessControlAttributeConfiguration	授予为 ABAC 启用实例并指定属性的权限	写入	Instance*		iam:AttachRolePolicy iam:CreateRole iam:DeleteRole iam:DeleteRolePolicy iam:DetachRolePolicy iam:GetRole iam:ListAttachedRolePolicies iam:ListRolePolicies iam:PutRolePolicy iam:UpdateAssumeRolePolicy

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateManagedApplicationInstance	授予向 Amazon IAM 身份中心添加托管应用程序实例的权限	写入			
CreatePermissionSet	授予权限以创建权限集	Write	Instance*		
			PermissionSet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfile	授予权限以为应用程序实例创建配置文件	Write			
CreateTrust	授予权限以在目标账户中创建联合信任	写入			
CreateTrustedTokenIssuer	授予为实例创建可信令牌颁发机构的权限	写入	Instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccountAssignment	授予 Amazon Web Services 账户 使用指定权限集删除委托人访问权限的权限	写入	Account*		
			Instance*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			PermissionSet*		
DeleteApplication	授予删除应用程序的权限	写入	Application*		
				sso:ApplicationAccount	
DeleteApplicationAccessScope	授予删除应用程序的访问范围的权限	写入	Application*		
				sso:ApplicationAccount	
DeleteApplicationAssignment	授予删除应用程序分配的权限	写入	Application*		
				sso:ApplicationAccount	
DeleteApplicationAuthenticationMethod	授予删除应用程序的身份验证方法的权限	写入	Application*		
				sso:ApplicationAccount	
DeleteApplicationGrant	授予删除来自应用程序的授权的权限	写入	Application*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				sso:ApplicationAccount	
DeleteApplicationInstance	授予权限以删除应用程序实例	Write			
DeleteApplicationInstanceCertificate	授予权限以删除应用程序实例的停用或过期证书	写入			
DeleteInlinePolicyFromPermissionSet	授予权限以从指定权限集中删除内联策略	写入	Instance*		
			PermissionSet*		
DeleteInstance	授予删除 Identity Center 实例的权限	写入	Instance*		
DeleteInstanceAccessControlAttributeConfiguration	授予禁用 ABAC 并删除实例属性列表的权限	Write	Instance*		
DeleteManagedApplicationInstance	授予权限以删除托管应用程序实例	Write			
DeletePermissionSet	授予权限以删除权限集	写入	Instance*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			PermissionSet*		
DeletePermissionsBoundaryFromPermissionSet	授予权限以从权限集中删除权限边界	权限管理	Instance*		
			PermissionSet*		
DeletePermissionsPolicy	授予权限以删除与权限集关联的权限策略	Permissions management			
DeleteProfile	授予权限以删除应用程序实例的配置文件	写入			
DeleteTrustedTokenIssuer	授予删除实例的可信令牌颁发机构的权限	写入	TrustedTokenIssuer*		
DescribeAccountAssignmentCreationStatus	授予权限以描述分配创建请求的状态	读取	Instance*		
DescribeAccountAssignmentDeletionStatus	授予权限以描述分配删除请求的状态	读取	Instance*		
DescribeApplication	授予获取应用程序信息的权限	读取	Application*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				sso:ApplicationAccount	
DescribeApplicationAssignment	授予检索应用程序分配的权限	读取	Application*		
				sso:ApplicationAccount	
DescribeApplicationProvider	授予描述应用程序提供者的权限	读取	ApplicationProvider*		
DescribeDirectories	授予获取此账户的目录相关信息的权限	读取			
DescribeInstance	授予获取 Identity Center 实例信息的权限	读取	Instance*		
DescribeInstanceAccessControlAttributeConfiguration	授予获取用于 ABAC 实例的属性列表的权限	Read	Instance*		
DescribePermissionSet	授予权限以描述权限集	读取	Instance*		
			PermissionSet*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribePermissionSetProvisioningStatus	授予权限以描述给定权限集预置请求的状态	读取	Instance*		
DescribePermissionsPolicies	授予权限以检索与某一权限集合关联的所有权限策略	读取			
DescribeRegisteredRegions	授予权限以获取您的组织已启用 Amazon IAM 身份中心的区域	读取			
DescribeTrustedTokenIssuer	授予描述实例的可信令牌颁发机构的权限	读取	TrustedTokenIssuer*		
DescribeTrusts	授予获取此账户的信任关系的相关信息的权限	读取			
DetachCustomerManagedPolicyReferenceFromPermissionSet	授予权限以将客户管理型策略参考从权限集分离	权限管理	Instance* PermissionSet*		
DetachManagedPolicyFromPermissionSet	授予将附加的 Amazon 托管策略与指定权限集分开的权限	权限管理	Instance* PermissionSet*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DisassociateDirectory	授予解除与 Amazon IAM 身份中心使用的目录关联的权限	写入			ds:UnauthorizeApplication
DisassociateProfile	授予权限以取消目录用户或组与配置文件的关联	写入			
GetApplicationAccessScope	授予获取应用程序的访问范围的权限	读取	Application*		
				sso:ApplicationAccount	
GetApplicationAssignmentConfiguration	授予读取应用程序的分配配置的权限	读取	Application*		
				sso:ApplicationAccount	
GetApplicationAuthenticationMethod	授予获取应用程序的身份验证方法的权限	读取	Application*		
				sso:ApplicationAccount	
GetApplicationGrant	授予获取属于应用程序的授权的详细信息的权限	读取	Application*		
				sso:ApplicationAccount	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetApplicationInstance	授予权限以检索应用程序实例的详细信息	Read			
GetApplicationTemplate	授予权限以检索应用程序模板详细信息	读取			
GetInlinePolicyForPermissionSet	授予权限以获取分配给权限集的内联策略	读取	Instance*		
			PermissionSet*		
GetManagedApplicationInstance	授予权限以检索应用程序实例的详细信息	Read			
GetMfaDeviceManagementForDirectory	授予权限以检索目录的 MFA 设备管理设置	Read			
GetPermissionSet	授予权限以检索权限集的详细信息	读取			
GetPermissionsBoundaryForPermissionSet	授予权限以获取权限集的权限边界	读取	Instance*		
			PermissionSet*		
GetPermissionsPolicy	授予权限以检索与权限集关联的所有权限策略	Read			sso:DescribePermissionsPolicies

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetProfile	授予权限以检索应用程序实例的配置文件	读取			
GetSSOStatus	授予权限以检查是否已启用 Amazon IAM 身份中心	读取			
GetSharedSsoConfiguration	授予权限以检索当前 SSO 实例的共享配置	Read			
GetSsoConfiguration	授予权限以检索当前 SSO 实例的配置	Read			
GetTrust	授予权限以检索目标账户中的联合信任	Read			
ImportApplicationInstanceServiceProviderMetadata	授予权限以上传服务提供商提供的应用程序 SAML 元数据文件，从而更新应用程序实例	写入			
ListAccountAssignmentCreationStatus	授予列出指定 SSO Amazon Web Services 账户 实例的任务创建请求状态的权限	列表	Instance*		
ListAccountAssignmentDeletionStatus	授予列出指定 SSO Amazon Web Services 账户 实例的任务删除请求状态的权限	列表	Instance*		
ListAccountAssignments	授予列出 Amazon Web Services 账户 具有指定权限集的指定受让人的权限	列表	Account* Instance*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			PermissionSet*		
ListAccountAssignmentsForPrincipal	授予列出分配给用户或组的账户的权限	列表	Instance*		
ListAccountsForProvisionedPermissionSet	授予列出所有配置了指定权限集的 Amazon 账户的权限	列表	Instance*		
			PermissionSet*		
ListApplicationAccessScopes	授予列出应用程序的访问范围的权限	列表	Application*		
				sso:ApplicationAccount	
ListApplicationAssignments	授予列出应用程序分配的权限	列表	Application*		
				sso:ApplicationAccount	
ListApplicationAssignmentsForPrincipal	授予列出分配给用户或组的应用程序的权限	列表	Instance*		
				sso:ApplicationAccount	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListApplicationAuthenticationMethods	授予列出应用程序的身份验证方法的权限	列表	Application*		
				sso:ApplicationAccount	
ListApplicationGrants	授予列出来自应用程序的授权的权限	列表	Application*		
				sso:ApplicationAccount	
ListApplicationInstanceCertificates	授予权限以检索给定应用程序实例的所有证书	Read			
ListApplicationInstances	授权权限以检索所有应用程序实例	列表			sso:GetApplicationInstance
ListApplicationProviders	授予列出应用程序提供者的权限	列表	ApplicationProvider*		
ListApplicationTemplates	授予权限以检索所有支持的应用程序模板	列表			sso:GetApplicationTemplate
ListApplications	授予检索与 IAM Identity Center 实例关联的所有应用程序的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListCustomerManagedPolicyReferencesInPermissionSet	授予权限以列出附加到权限集的客户管理型策略参考	列表	Instance* PermissionSet*		
ListDirectoryAssociations	授予权限以检索与 Amazon IAM 身份中心连接的目录的详细信息	读取			
ListInstances	授予权限以列出发起人有权访问的 SSO 实例	列表			
ListManagedPoliciesInPermissionSet	授予列出附加到指定权限集的 Amazon 托管策略的权限	列表	Instance* PermissionSet*		
ListPermissionSetProvisioningStatus	授予权限以列出指定 SSO 实例的权限集预置请求的状态	列表	Instance*		
ListPermissionSets	授予权限以检索所有权限集	列表	Instance*		
ListPermissionSetsProvisionedToAccount	授予列出配置给指定的所有权限集的权限 Amazon Web Services 账户	列表	Account* Instance*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListProfileAssociations	授予权限以检索与配置文件关联的目录用户或组	Read			
ListProfiles	授予权限以检索应用程序实例的所有配置文件	列表			sso:GetProfile
ListTagsForResource	授予权限以列出附加到指定资源的标签	读取	Application		
			Instance		
			PermissionSet		
			TrustedTokenIssuer		
ListTrustedTokenIssuers	授予列出实例的可信令牌颁发机构的权限	列表	Instance*		
ProvisionPermissionSet	授予权限以将指定权限集预置到指定目标	写入	Account*		
			Instance*		
			PermissionSet*		
PutApplicationAccessScope	授予创建/更新应用程序的访问范围的权限	写入	Application*		
				sso:ApplicationAccount	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutApplicationAssignmentConfiguration	授予向应用程序添加分配配置的权限	写入	Application*		
				sso:ApplicationAccount	
PutApplicationAuthenticationMethod	授予创建/更新应用程序的身份验证方法的权限	写入	Application*		
				sso:ApplicationAccount	
PutApplicationGrant	授予创建/更新对应用程序的授权的权限	写入	Application*		
				sso:ApplicationAccount	
PutInlinePolicyToPermissionSet	授予权限以将 IAM 内联策略附加到权限集	写入	Instance*		
			PermissionSet*		
PutMfaDeviceManagementForDirectory	授予权限以为目录附加 MFA 设备管理设置	写入			
PutPermissionsBoundaryToPermissionSet	授予权限以将权限边界添加到权限集	权限管理	Instance*		
			PermissionSet*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutPermissionsPolicy	授予权限以将策略添加到权限集	Permissions management			
SearchGroups	授予权限以在关联的目录中搜索组	Read			ds:DescribeDirectories
SearchUsers	授予权限以在关联的目录中搜索用户	读取			ds:DescribeDirectories
StartSSO	授予初始化 Amazon IAM 身份中心的权限	写入			organizations:DescribeOrganization organizations:EnableAWSServiceAccess
TagResource	授予权限以将一组标签与指定资源关联	标记	Application		
			Instance		
			PermissionSet		
			TrustedTokenIssuer		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予权限以取消一组标签与指定资源的关联	标记	Application		
			Instance		
			PermissionSet		
			TrustedTokenIssuer		
				aws:TagKeys	
UpdateApplication	授予更新应用程序的权限	写入	Application*		
				sso:ApplicationAccount	
UpdateApplicationInstanceActiveCertificate	授予权限以为此应用程序实例设置证书，作为活动证书	Write			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateApplicationInstanceDisplayData	授予权限以更新应用程序实例的显示数据	Write			
UpdateApplicationInstanceResponseConfiguration	授予权限以更新应用程序实例的联合响应配置	Write			
UpdateApplicationInstanceResponseSchemaConfiguration	授予权限以更新应用程序实例的联合响应架构配置	Write			
UpdateApplicationInstanceSecurityConfiguration	授予权限以更新应用程序实例的安全详细信息	Write			
UpdateApplicationInstanceServiceProviderConfiguration	授予权限以更新应用程序实例的服务提供商关联配置	Write			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateApplicationInstanceStatus	授予权限以更新应用程序实例的状态	Write			
UpdateDirectoryAssociation	授予权限以更新连接目录的用户属性映射	写入			
UpdateInstance	授予更新 Identity Center 实例的权限	写入	Instance*		
UpdateInstanceAccessControlAttributeConfiguration	授予更新用于 ABAC 实例的属性的权限	Write	Instance*		
UpdateManagedApplicationInstanceStatus	授予权限以更新托管应用程序的实例状态	写入			
UpdatePermissionSet	授予权限以更新权限集	权限管理	Instance*		
			PermissionSet*		
UpdateProfile	授予权限以更新应用程序实例的配置文件	Write			
UpdateSSOConfiguration	授予权限以更新当前 SSO 实例的配置	Write			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateTrust	授予权限以更新目标账户中的联合信任	写入			
UpdateTrustedTokenIssuer	授予更新实例的可信令牌颁发机构的权限	写入	TrustedTokenIssuer *		

由 Amazon IAM 身份中心（ Amazon 单点登录的继任者）定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
PermissionSet	arn:${Partition}:sso:::permissionSet/${InstanceId}/${PermissionSetId}	aws:ResourceTag/${TagKey}
Account	arn:${Partition}:sso:::account/${AccountId}	
Instance	arn:${Partition}:sso:::instance/${InstanceId}	aws:ResourceTag/${TagKey}
Application	arn:${Partition}:sso::${AccountId}:application/${InstanceId}/${ApplicationId}	aws:ResourceTag/${TagKey} sso:ApplicationAccount
TrustedTokenIssuer	arn:${Partition}:sso::${AccountId}:trustedTokenIssuer/${InstanceId}/${TrustedTokenIssuerId}	aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
ApplicationProvider	arn:${Partition}:sso::aws:applicationProvider/${ApplicationProviderId}	

Amazon IAM 身份中心（ Amazon 单点登录的继任者）的条件密钥

Amazon IAM Identity Center（ Amazon 单点登录的继任者）定义了以下条件密钥，这些条件密钥可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString
sso:ApplicationAccount	按创建应用程序的账户筛选访问权限	字符串

Amazon IAM Identity Center（ Amazon 单点登录的继任者）目录的操作、资源和条件密钥

Amazon IAM Identity Center（ Amazon 单点登录的继任者sso-directory）目录（服务前缀:）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。

- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

由 Amazon IAM 身份中心（ Amazon 单点登录的继任者）目录定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddMemberToGroup	授予将成员添加到 Amazon IAM Identity Center 默认提供的目录中的群组的权限	写入			
CompleteVirtualMfaDeviceRegistration	授予权限以完成虚拟 MFA 设备的创建过程	写入			
CompleteWebAuthnDeviceRegistration	授予完成 WebAuthn 设备注册过程的权限	写入			
CreateAlias	授予为 Amazon IAM 身份中心默认提供的目录创建别名的权限	写入			
CreateBearerToken	授予权限以便为给定的预置租户创建持有者令牌	Write			
CreateExternalIdPConfigurationForDirectory	授予权限以便为目录创建外部身份提供商配置	写入			
CreateGroup	授予在 Amazon IAM 身份中心默认提供的目录中创建群组的权限	写入			
CreateProvisioningTenant	授予权限以便为给定的目录创建预置租户	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateUser	授予在 Amazon IAM 身份中心默认提供的目录中创建用户的权限	写入			
DeleteBearerToken	授予权限以删除持有者令牌	Write			
DeleteExternalIdPCertificate	授予权限以删除给定的外部 IdP 证书	Write			
DeleteExternalIdPConfigurationForDirectory	授予权限以删除与目录关联的外部身份提供商配置	写入			
DeleteGroup	授予从 Amazon IAM 身份中心默认提供的目录中删除群组的权限	写入			
DeleteMfaDeviceForUser	授予权限以按设备名称删除给定用户的 MFA 设备	Write			
DeleteProvisioningTenant	授予权限以删除预置租户	写入			
DeleteUser	授予从 Amazon IAM 身份中心默认提供的目录中删除用户的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeDirectory	授予权限以检索 Amazon IAM 身份中心默认提供的目录的相关信息	读取			
DescribeGroup	授予权限以查询组数据，不包括用户和组成员	读取			
DescribeGroups	授予从 Amazon IAM Identity Center 默认提供的目录中检索群组信息的权限	读取			
DescribeProvisioningTenant	授予权限以描述预置租户	读取			
DescribeUser	授予从 Amazon IAM 身份中心默认提供的目录中检索用户信息的权限	读取			
DescribeUserByUniqueAttribute	授予权限以使用代表用户的有效唯一属性描述用户	读取			
DescribeUsers	授予从 Amazon IAM Identity Center 默认提供的目录中检索用户信息的权限	读取			
DisableExternalIdPConfigurationForDirectory	授予权限以禁止最终用户使用外部身份提供商进行身份验证	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DisableUser	授予在 Amazon IAM 身份中心默认提供的目录中停用用户的权限	写入			
EnableExternalIdPConfigurationForDirectory	授予权限以允许最终用户使用外部身份提供商进行身份验证	写入			
EnableUser	授予在 Amazon IAM 身份中心默认提供的目录中激活用户的权限	写入			
GetAWSSPConfigurationForDirectory	授予检索目录的 Amazon IAM 身份中心服务提供商配置的权限	读取			
GetGroupId	授予从 Amazon IAM 身份中心默认提供的目录中检索有关群组的 ID 信息的权限	读取			
GetUserId	授予从 Amazon IAM 身份中心默认提供的目录中检索用户 ID 信息的权限	读取			
GetUserPoolInfo	（已弃用）授予获取 UserPool 信息的权限	读取			
ImportExternalIdPCertificate	授予权限以导入用于验证外部 IdP 响应的 IdP 证书	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
IsMemberInGroup	授予权限以检查成员是否是 Amazon IAM Identity Center 默认提供的目录中群组的成员	读取			
IsMemberInGroups	授予权限以检查成员是否属于 Amazon IAM Identity Center 默认提供的目录中多个群组的成员	读取			
ListBearerTokens	授予权限以列出给定预置租户的持有者令牌	Read			
ListExternalIdPCertificates	授予权限以列出给定目录和 IdP 的外部 IdP 证书	Read			
ListExternalIdPConfigurationsForDirectory	授予权限以列出为目录创建的所有外部身份提供商配置	读取			
ListGroups	授予从 Amazon IAM 身份中心默认提供的目录中列出群组的权限	读取			
ListGroupsForMember	授予权限以列出目标成员组	读取			
ListGroupsForUser	授予从 Amazon IAM 身份中心默认提供的目录中为用户列出群组的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListMembersInGroup	授予权限以检索 Amazon IAM Identity Center 默认提供的目录中属于群组的所有成员	读取			
ListMfaDevicesForUser	授予权限以列出用户的所有活动 MFA 设备及其 MFA 设备元数据	Read			
ListProvisioningTenants	授予权限以列出给定目录的预置租户	读取			
ListUsers	授予从 Amazon IAM 身份中心默认提供的目录中列出用户的权限	读取			
RemoveMemberFromGroup	授予删除属于 Amazon IAM Identity Center 默认提供的目录中群组成员的权限	写入			
SearchGroups	授予权限以在关联的目录中搜索组	Read			
SearchUsers	授予权限以在关联的目录中搜索用户	Read			
StartVirtualMfaDeviceRegistration	授予权限以开始虚拟 mfa 设备的创建过程	写入			
StartWebAuthnDeviceRegistration	授予开始 WebAuthn 设备注册过程的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateExternalIdPConfigurationForDirectory	授予权限以更新与目录关联的外部身份提供商配置	写入			
UpdateGroup	授予权限以更新 Amazon IAM Identity Center 默认提供的目录中群组的信息	写入			
UpdateGroupDisplayName	授予权限以更新组显示名称更新组显示名称响应	Write			
UpdateMfaDeviceForUser	授予更新 MFA 设备信息的权限	写入			
UpdatePassword	通过电子邮件发送密码重置链接或在 Amazon IAM Identity Center 默认提供的目录中为用户生成一次性密码，授予更新密码的权限	写入			
UpdateUser	授予更新 Amazon IAM 身份中心默认提供的目录中的用户信息的权限	写入			
UpdateUserName	授予权限以更新用户名更新用户名响应	Write			
VerifyEmail	授予权限以验证用户的电子邮件地址	写入			

由 Amazon IAM 身份中心（ Amazon 单点登录的继任者）目录定义的资源类型

Amazon IAM 身份中心（ Amazon 单点登录的继任者）目录不支持在 IAM 策略声明的元素`Resource`中指定资源 ARN。要允许访问 Amazon IAM Identity Center（ Amazon 单点登录的继任者）目录，请在策略`"Resource": "*"`中指定。

Amazon IAM 身份中心（ Amazon 单点登录的继任者）目录的条件密钥

IAM Identity Center（ Amazon SSO 的继任者）目录没有可在策略声明`Condition`元素中使用的特定于服务的上下文密钥。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon IAM Identity Center OIDC 服务的操作、资源和条件键

Amazon IAM Identity Center OIDC 服务（服务前缀:`sso-oauth`）提供以下特定于服务的资源、操作和条件上下文密钥以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon IAM Identity Center OIDC 服务定义的操作
- Amazon IAM Identity Center OIDC 服务定义的资源类型
- Amazon IAM Identity Center OIDC 服务的条件键

Amazon IAM Identity Center OIDC 服务定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须

具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateTokenWithIAM	授予创建 OAuth /OIDC 令牌以访问 IAM 身份中心集成应用程序的权限	写入	Application*		

Amazon IAM Identity Center OIDC 服务定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
Application	arn:${Partition}:sso::${AccountId}:application/${InstanceId}/${ApplicationId}	

Amazon IAM Identity Center OIDC 服务的条件键

OIDC 服务没有可以在策略语句的 Condition 元素中使用的服务特定上下文键。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon Identity and Access Management（IAM）的操作、资源和条件键

Amazon Identity and Access Management (IAM)（服务前缀iam:）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Identity and Access Management（IAM）定义的操作
- Amazon Identity and Access Management（IAM）定义的资源类型
- Amazon Identity and Access Management（IAM）的条件键

Amazon Identity and Access Management（IAM）定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddClientIDToOpenIDConnectProvider	授予将新客户端 ID（受众）添加到指定 IAM OpenID Connect (OIDC) IDs 提供商资源的注册列表的权限	写入	oidc-provider*		
AddRoleToInstanceProfile	授予权限以将 IAM 角色添加到指定的实例配置文件中	Write	instance-profile*		iam:PassRole
AddUserToGroup	授予权限以将 IAM 用户添加到指定的 IAM 组中	Write	group*		
AttachGroupPolicy	授予权限以将托管策略附加到指定的 IAM 组	Permissions management	group*		
				iam:PolicyARN	
AttachRolePolicy	授予权限以将托管策略附加到指定的 IAM 角色	Permissions management	role*		
				iam:PolicyARN iam:PermissionsBoundary	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AttachUserPolicy	授予权限以将托管策略附加到指定的 IAM 用户	权限管理	user*		
				iam:PolicyARN iam:PermissionsBoundary	
ChangePassword	授予 IAM 用户更改自己密码的权限	写入	user*		
CreateAccessKey	授予权限以便为指定 IAM 用户创建访问密钥和秘密访问密钥	写入	user*		
CreateAccountAlias	授予为你创建别名的权限 Amazon Web Services 账户	写入			
CreateGroup	授予权限以创建新的组	Write	group*		
CreateInstanceProfile	授予权限以创建新的实例配置文件	Write	instance-profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateLoginProfile	授予权限以便为指定的 IAM 用户创建密码	Write	user*		
CreateOpenIDConnectProvider	授予权限以创建 IAM 资源，它描述支持 OpenID Connect (OIDC) 的身份提供商 (IdP)	Write	oidc-provider*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePolicy	授予权限以创建新的托管策略	Permissions management	policy*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePolicyVersion	授予权限以创建指定托管策略的新版本	Permissions management	policy*		
CreateRole	授予权限以创建新的角色	Write	role*		
				iam:PermissionsBoundary aws:TagKeys aws:RequestTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateSAMLProvider	授予权限以创建 IAM 资源，它描述支持 SAML 2.0 的身份提供商 (IdP)	写入	saml-provider*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateServiceLinkedRole	授予创建 IAM 角色的权限，该角色允许 Amazon 服务代表您执行操作	写入	role*		
				iam:AWSServiceName	
CreateServiceSpecificCredential	授予权限以便为 IAM 用户创建新的服务特定凭证	Write	user*		
CreateUser	授予权限以创建新的 IAM 用户	Write	user*		
				iam:PermissionsBoundary aws:TagKeys aws:RequestTag/${TagKey}	
CreateVirtualMFADevice	授予权限以创建新的虚拟 MFA 设备	Write	mfa*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys aws:RequestTag/${TagKey}	
DeactivateMFADevice	授予权限以停用指定的 MFA 设备，并删除最初启用了该设备的 IAM 用户与其之间的关联	Write	user*		
DeleteAccessKey	授予权限以删除与指定 IAM 用户关联的访问密钥对	写入	user*		
DeleteAccountAlias	授予删除指定 Amazon Web Services 账户 别名的权限	写入			
DeleteAccountPasswordPolicy	授予删除密码策略的权限 Amazon Web Services 账户	权限管理			
DeleteCloudFrontPublicKey	授予删除现有 CloudFront 公钥的权限	写入			
DeleteGroup	授予权限以删除指定的 IAM 组	Write	group*		
DeleteGroupPolicy	授予权限以将指定的内联策略从其组中删除	Permissions management	group*		
DeleteInstanceProfile	授予权限以删除指定的实例配置文件	Write	instance-profile*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteLoginProfile	授予权限以删除指定 IAM 用户的密码	Write	user*		
DeleteOpenIDConnectProvider	授予权限以在 IAM 中删除 OpenID Connect 身份提供商 (IdP) 资源对象	Write	oidc-provider*		
DeletePolicy	授予权限以删除指定的托管策略，并将其从附加到的任何 IAM 实体（用户、组或角色）中删除	Permissions management	policy*		
DeletePolicyVersion	授予权限以从指定的托管策略中删除版本	Permissions management	policy*		
DeleteRole	授予权限以删除指定的角色	Write	role*		
DeleteRolePermissionsBoundary	授予权限以从角色中删除权限边界	Permissions management	role*		
				iam:PermissionsBoundary	
DeleteRolePolicy	授予权限以从指定的角色中删除指定的内联策略	Permissions management	role*		
				iam:PermissionsBoundary	
DeleteSAMLProvider	授予权限以在 IAM 中删除 SAML 提供程序资源	Write	saml-provider*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteSSHPublicKey	授予权限以删除指定的 SSH 公有密钥	Write	user*		
DeleteServerCertificate	授予权限以删除指定的服务器证书	写入	server-certificate*		
DeleteServiceLinkedRole	如果该服务已停止使用 IAM 角色，则授予删除与该 Amazon 服务关联的 IAM 角色的权限	写入	role*		
DeleteServiceSpecificCredential	授予权限以删除 IAM 用户的指定服务特定凭证	Write	user*		
DeleteSigningCertificate	授予权限以删除与指定 IAM 用户关联的签名证书	Write	user*		
DeleteUser	授予权限以删除指定的 IAM 用户	Write	user*		
DeleteUserPermissionsBoundary	授予权限以从指定的 IAM 用户中删除权限边界	Permissions management	user*		
				iam:PermissionsBoundary	
DeleteUserPolicy	授予权限以从 IAM 用户中删除指定的内联策略	Permissions management	user*		
				iam:PermissionsBoundary	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteVirtualMFADevice	授予权限以删除虚拟 MFA 设备	Write	mfa		
			sms-mfa		
DetachGroupPolicy	授予权限以将托管策略从指定的 IAM 组中分离	Permissions management	group*		
				iam:PolicyARN	
DetachRolePolicy	授予权限以将托管策略从指定的角色中分离	Permissions management	role*		
				iam:PolicyARN iam:PermissionsBoundary	
DetachUserPolicy	授予权限以将托管策略从指定的 IAM 用户中分离	权限管理	user*		
				iam:PolicyARN iam:PermissionsBoundary	
DisableOrganizationsRootCredentialsManagement	授予权限以禁用当前账户管理的组织的成员账户 root 用户凭证的管理	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DisableOrganizationsRootSessions	授予在当前账户下管理的组织的成员账户中禁用特权 root 操作的权限	写入			
EnableMFADevice	授予权限以启用 MFA 设备，并将其与指定的 IAM 用户相关联	写入	user*		
				iam:RegisterSecurityKey iam:FIDO-FIPS-140-2-certification iam:FIDO-FIPS-140-3-certification iam:FIDO-certification	
EnableOrganizationsRootCredentialsManagement	授予允许管理当前账户下管理的组织的成员账户 root 用户凭证的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
EnableOrganizationsRootSessions	授予在当前账户下管理的组织的成员账户中启用特权 root 操作的权限	写入			
GenerateCredentialReport	授予生成证书报告的权限 Amazon Web Services 账户	读取			
GenerateOrganizationsAccessReport	授予为 Organizations 实体生成访问报告的权限 Amazon	读取	access-report*		organizations:DescribePolicy organizations:ListChildren organizations:ListParents organizations:ListPoliciesForTarget organizations:ListRoots organizations:ListTargetsForPolicy

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				iam:OrganizationsPolicyId	
GenerateServiceLastAccessedDetails	授予权限以便为 IAM 资源生成上次访问的服务数据报告	Read	group*		
			policy*		
			role*		
			user*		
GetAccessKeyLastUsed	授予权限以检索有关上次使用指定访问密钥的时间的信息	读取	user*		
GetAccountAuthorizationDetails	授予权限以检索有关您的所有 IAM 用户、群组、角色和策略的信息 Amazon Web Services 账户，包括他们之间的关系	读取			
GetAccountEmailAddress	授予检索与账户关联的电子邮件地址的权限	读取			
GetAccountName	授予检索与账户关联的账户名称的权限	读取			
GetAccountPasswordPolicy	授予检索密码策略的权限 Amazon Web Services 账户	读取			
GetAccountSummary	授予在中检索有关 IAM 实体使用情况和 IAM 配额信息的权限 Amazon Web Services 账户	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetCloudFrontPublicKey	授予检索有关指定 CloudFront 公钥信息的权限	读取			
GetContextKeysForCustomPolicy	授予权限以检索指定策略中引用的所有上下文键的列表	Read			
GetContextKeysForPrincipalPolicy	授予权限以检索附加到指定 IAM 身份（用户、组或角色）的所有 IAM policy 中引用的所有上下文键的列表	读取	group		
			role		
			user		
GetCredentialReport	授予检索证书报告的权限 Amazon Web Services 账户	读取			
GetGroup	授予权限以检索指定 IAM 组中的 IAM 用户列表	Read	group*		
GetGroupPolicy	授予权限以检索嵌入在指定 IAM 组中的内联策略文档	Read	group*		
GetInstanceProfile	授予权限以检索有关指定实例配置文件的信息，包括实例配置文件的路径、GUID、ARN 和角色	Read	instance-profile*		
GetLoginProfile	授予权限以检索指定 IAM 用户的用户名和密码创建日期	列表	user*		
GetMFADevice	授予检索指定的用户 MFA 设备相关信息的权限	读取	user*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetOpenIDConnectProvider	授予权限以在 IAM 中检索有关指定 OpenID Connect (OIDC) 提供商资源的信息	读取	oidc-provider*		
GetOrganizationsAccessReport	授予检索 Organizati Amazon ons 访问报告的权限	读取			
GetPolicy	授予权限以检索有关指定托管策略的信息，包括策略的默认版本以及策略附加到的身份总数	Read	policy*		
GetPolicyVersion	授予权限以检索有关指定托管策略的版本的信息，包括策略文档	Read	policy*		
GetRole	授予权限以检索有关指定角色的信息，包括角色的路径、GUID、ARN 和角色的信任策略	Read	role*		
GetRolePolicy	授予权限以检索嵌入在指定 IAM 角色中的内联策略文档	Read	role*		
GetSAMLProvider	授予权限以检索在创建或更新 IAM SAML 提供商资源时上传的 SAML 提供商元文档	Read	saml-provider*		
GetSSHPublicKey	授予权限以检索指定的 SSH 公有密钥，包括有关密钥的元数据	Read	user*		
GetServerCertificate	授予权限以检索有关 IAM 中存储的指定服务器证书的信息	Read	server-certificate*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetServiceLastAccessedDetails	授予权限以检索有关上次访问的服务数据报告的信息	Read			
GetServiceLastAccessedDetailsWithEntities	授予权限以从上次访问的服务数据报告中检索有关实体的信息	Read			
GetServiceLinkedRoleDeletionStatus	授予权限以检索 IAM 服务相关角色删除状态	Read	role*		
GetUser	授予权限以检索有关指定 IAM 用户的信息，包括用户的创建日期、路径、唯一 ID 和 ARN	Read	user*		
GetUserPolicy	授予权限以检索嵌入在指定 IAM 用户中的内联策略文档	读取	user*		
ListAccessKeys	授予权限以列出与指定 IAM 用户关联的访问密钥 IDs 的相关信息	列表	user*		
ListAccountAliases	授予列出与关联的账户别名的权限 Amazon Web Services 账户	列表			
ListAttachedGroupPolicies	授予权限以列出附加到指定 IAM 组的所有托管策略	List	group*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListAttachedRolePolicies	授予权限以列出附加到指定 IAM 角色的所有托管策略	List	role*		
ListAttachedUserPolicies	授予权限以列出附加到指定 IAM 用户的所有托管策略	列表	user*		
ListCloudFrontPublicKeys	授予列出该账户所有当前 CloudFront 公钥的权限	列表			
ListEntitiesForPolicy	授予权限以列出指定托管策略附加到的所有 IAM 身份	List	policy*		
ListGroupPolicies	授予权限以列出嵌入在指定 IAM 组中的内联策略的名称	List	group*		
ListGroups	授予权限以列出具有指定路径前缀的 IAM 组	List			
ListGroupsForUser	授予权限以列出指定 IAM 用户所属的 IAM 组	List	user*		
ListInstanceProfileTags	授予权限以列出附加到指定实例配置文件的标签	List	instance-profile*		
ListInstanceProfiles	授予权限以列出具有指定路径前缀的实例配置文件	List			
ListInstanceProfilesForRole	授予权限以列出具有指定的关联 IAM 角色的实例配置文件	List	role*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListMFADeviceTags	授予权限以列出附加到指定虚拟 MFA 设备的标签	List	mfa*		
ListMFADevices	授予权限以列出 IAM 用户的 MFA 设备	List	user		
ListOpenIDConnectProviderTags	授予权限以列出附加到指定 OpenID Connect 提供商的标签	列表	oidc-provider*		
ListOpenIDConnectProviders	授予列出有关在 IAM OpenID Connect (OIDC) 提供商资源对象中定义的信息的权限 Amazon Web Services 账户	列表			
ListOrganizationsFeatures	授予列出为组织启用的集中根访问功能的权限	列表			
ListPolicies	授予权限以列出所有托管策略	List			
ListPoliciesGrantingServiceAccess	授予权限以列出有关为实体授予特定服务的访问权限的策略的信息	List	group*		
			role*		
			user*		
ListPolicyTags	授予权限以列出附加到指定托管策略的标签	List	policy*		
ListPolicyVersions	授予权限以列出有关指定托管策略的版本的信息，包括当前设置为策略默认版本的版本	List	policy*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListRolePolicies	授予权限以列出嵌入在指定 IAM 角色中的内联策略的名称	List	role*		
ListRoleTags	授予权限以列出附加到指定 IAM 角色的标签	List	role*		
ListRoles	授予权限以列出具有指定路径前缀的 IAM 角色	List			
ListSAMLProviderTags	授予权限以列出附加到指定 SAML 提供商的标签	List	saml-provider*		
ListSAMLProviders	授予权限以列出 IAM 中的 SAML 提供商资源	List			
ListSSHPublicKeys	授予权限以列出有关与指定 IAM 用户关联的 SSH 公有密钥的信息	列表	user*		
ListSTSRegionalEndpointsStatus	授予列出所有活动 STS 区域端点状态的权限	列表			
ListServerCertificateTags	授予权限以列出附加到指定服务器证书的标签	List	server-certificate*		
ListServerCertificates	授予权限以列出具有指定路径前缀的服务器证书	List			
ListServiceSpecificCredentials	授予权限以列出与指定 IAM 用户关联的服务特定凭证	List	user*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListSigningCertificates	授予权限以列出有关与指定 IAM 用户关联的签名证书的信息	List	user*		
ListUserPolicies	授予权限以列出嵌入在指定 IAM 用户中的内联策略的名称	List	user*		
ListUserTags	授予权限以列出附加到指定 IAM 用户的标签	List	user*		
ListUsers	授予权限以列出具有指定路径前缀的 IAM 用户	List			
ListVirtualMFADevices	授予权限以按分配状态列出虚拟 MFA 设备	List			
PassRole[仅权限]	授予权限以将角色传递给服务	Write	role*		
				iam:AssociatedResourceArn iam:PassedToService	
PutGroupPolicy	授予权限以创建或更新嵌入在指定 IAM 组中的内联策略文档	Permissions management	group*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutRolePermissionsBoundary	授予权限以将托管策略设置为角色的权限边界	Permissions management	role*		
				iam:PermissionsBoundary	
PutRolePolicy	授予权限以创建或更新嵌入在指定 IAM 角色中的内联策略文档	Permissions management	role*		
				iam:PermissionsBoundary	
PutUserPermissionsBoundary	授予权限以将托管策略设置为 IAM 用户的权限边界	Permissions management	user*		
				iam:PermissionsBoundary	
PutUserPolicy	授予权限以创建或更新嵌入在指定 IAM 用户中的内联策略文档	权限管理	user*		
				iam:PermissionsBoundary	
RemoveClientIDFromOpenIDConnectProvider	授予从指定 IAM OpenID Connect (OIDC) 提供商资源的客户列表 IDs 中删除客户端 ID（受众）的权限	写入	oidc-provider*		
RemoveRoleFromInstanceProfile	授予从指定 EC2 实例配置文件中删除 IAM 角色的权限	写入	instance-profile*		
RemoveUserFromGroup	授予权限以从指定的组中删除 IAM 用户	Write	group*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ResetServiceSpecificCredential	授予权限以重置 IAM 用户的现有服务特定凭证的密码	Write	user*		
ResyncMFADevice	授予权限以将指定的 MFA 设备与其 IAM 实体（用户或角色）同步	Write	user*		
SetDefaultPolicyVersion	授予权限以将指定策略的版本设置为策略的默认版本	权限管理	policy*		
SetSTSRegionalEndpointStatus	授予激活或停用 STS 区域端点的权限	写入			
SetSecurityTokenServicePreferences	授予权限以设置 STS 全局终端节点令牌版本	Write			
SimulateCustomPolicy	授予权限以模拟基于身份的策略或基于资源的策略是否为特定 API 操作和资源提供权限	Read			
SimulatePrincipalPolicy	授予权限以模拟附加到指定 IAM 实体（用户或角色）的基于身份的策略是否为特定 API 操作和资源提供权限	Read	group		
			role		
			user		
TagInstanceProfile	授予权限以将标签添加到实例配置文件	Tagging	instance-profile*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys aws:RequestTag/${TagKey}	
TagMFADevice	授予权限以将标签添加到虚拟 MFA 设备	Tagging	mfa*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagOpenIDConnectProvider	授予权限以将标签添加到 OpenID Connect 提供商	Tagging	oidc-provider*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagPolicy	授予权限以将标签添加到托管策略	Tagging	policy*		
				aws:TagKeys aws:RequestTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
TagRole	授予权限以将标签添加到 IAM 角色	Tagging	role*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagSAMLProvider	授予权限以将标签添加到 SAML 提供商	Tagging	saml-provider*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagServerCertificate	授予权限以将标签添加到服务器证书	Tagging	server-certificate*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagUser	授予权限以将标签添加到 IAM 用户	Tagging	user*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagInstanceProfile	授予权限以从实例配置文件中删除指定的标签	Tagging	instance-profile*		
				aws:TagKeys	
UntagMFADevice	授予权限以从虚拟 MFA 设备中删除指定的标签	Tagging	mfa*		
				aws:TagKeys	
UntagOpenIDConnectProvider	授予权限以从 OpenID Connect 提供商中删除指定的标签	Tagging	oidc-provider*		
				aws:TagKeys	
UntagPolicy	授予权限以从托管策略中删除指定的标签	Tagging	policy*		
				aws:TagKeys	
UntagRole	授予权限以从角色中删除指定的标签	Tagging	role*		
				aws:TagKeys	
UntagSAMLProvider	授予权限以从 SAML 提供商中删除指定的标签	Tagging	saml-provider*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys	
UntagServerCertificate	授予权限以从服务器证书中删除指定的标签	Tagging	server-certificate*		
				aws:TagKeys	
UntagUser	授予权限以从用户中删除指定的标签	Tagging	user*		
				aws:TagKeys	
UpdateAccessKey	授予权限以将指定访问密钥的状态更新为活动或非活动状态	写入	user*		
UpdateAccountEmailAddress	授予更新与账户关联的电子邮件地址的权限	写入			
UpdateAccountName	授予更新与账户关联的账户名称的权限	写入			
UpdateAccountPasswordPolicy	授予更新密码策略设置的权限 Amazon Web Services 账户	写入			
UpdateAssumeRolePolicy	授予权限以更新为 IAM 实体授予权限以担任角色的策略	权限管理	role*		
UpdateCloudFrontPublicKey	授予更新现有 CloudFront 公钥的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateGroup	授予权限以更新指定 IAM 组的名称或路径	Write	group*		
UpdateLoginProfile	授予权限以更改指定 IAM 用户的密码	Write	user*		
UpdateOpenIDConnectProviderThumbprint	授予权限以更新与 OpenID Connect (OIDC) 提供商资源关联的服务器证书指纹的完整列表	Write	oidc-provider*		
UpdateRole	授予权限以更新角色的描述或最大会话持续时间设置	Write	role*		
UpdateRoleDescription	授予权限以仅更新角色描述	Write	role*		
UpdateSAMLProvider	授予权限以更新现有 SAML 提供商资源的元数据文档	Write	saml-provider*		
UpdateSSHPublicKey	授予权限以将 IAM 用户的 SSH 公有密钥状态更新为活动或非活动状态	Write	user*		
UpdateServerCertificate	授予权限以更新 IAM 中存储的指定服务器证书的名称或路径	Write	server-certificate*		
UpdateServiceSpecificCredential	授予权限以将 IAM 用户的服务特定凭证状态更新为活动或非活动状态	Write	user*		
UpdateSigningCertificate	授予权限以将指定用户签名证书的状态更新为活动或已禁用状态	Write	user*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateUser	授予权限以更新指定 IAM 用户的名称或路径	写入	user*		
UploadCloudFrontPublicKey	授予上传 CloudFront 公钥的权限	写入			
UploadSSHPublicKey	授予权限以上传 SSH 公有密钥，并将其与指定的 IAM 用户相关联	写入	user*		
UploadServerCertificate	授予上传服务器证书实体的权限 Amazon Web Services 账户	写入	server-certificate*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UploadSigningCertificate	授予权限以上传 X.509 签名证书，并将其与指定的 IAM 用户相关联	写入	user*		

Amazon Identity and Access Management（IAM）定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
access-report	arn:${Partition}:iam::${Account}:access-report/${EntityPath}	
assumed-role	arn:${Partition}:iam::${Account}:assumed-role/${RoleName}/${RoleSessionName}	
federated-user	arn:${Partition}:iam::${Account}:federated-user/${UserName}	
group	arn:${Partition}:iam::${Account}:group/${GroupNameWithPath}	
instance-profile	arn:${Partition}:iam::${Account}:instance-profile/${InstanceProfileNameWithPath}	aws:ResourceTag/${TagKey}
mfa	arn:${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}

资源类型	ARN	条件键
server-certificate	arn:${Partition}:iam::${Account}:server-certificate/${CertificateNameWithPath}	aws:ResourceTag/${TagKey}
sms-mfa	arn:${Partition}:iam::${Account}:sms-mfa/${MfaTokenIdWithPath}	
user	arn:${Partition}:iam::${Account}:user/${UserNameWithPath}	aws:ResourceTag/${TagKey} iam:ResourceTag/${TagKey}

Amazon Identity and Access Management（IAM）的条件键

Amazon 身份和访问管理 (IAM) 定义了以下条件密钥，这些条件键可用于 IAM 策略Condition的元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中传递的标签筛选访问	字符串
aws:ResourceTag/${TagKey}	根据与资源关联的标签筛选访问	字符串
aws:TagKeys	根据在请求中传递的标签键筛选访问	ArrayOfString
iam:AWSServiceName	筛选该角色所属 Amazon 服务的访问权限	字符串

条件键	描述	类型
iam:AssociatedResourceArn	按将代表使用的角色的资源筛选访问权限	ARN
iam:FIDO-FIPS-140-2-certification	按注册 FIDO 安全密钥时的 MFA 设备 FIPS-140-2 验证认证级别筛选访问权限	字符串
iam:FIDO-FIPS-140-3-certification	按注册 FIDO 安全密钥时的 MFA 设备 FIPS-140-3 验证认证级别筛选访问权限	字符串
iam:FIDO-certification	按注册 FIDO 安全密钥时的 MFA 设备 FIDO 认证级别筛选访问权限	字符串
iam:OrganizationsPolicyId	按 Organizations 策略的 Amazon ID 筛选访问权限	字符串
iam:PassedToService	筛选传递此角色的 Amazon 服务的访问权限	字符串
iam:PermissionsBoundary	根据指定策略设置是否为 IAM 实体（用户或角色）上的权限边界以筛选访问	ARN
iam:PolicyARN	按 IAM policy 的 ARN 筛选访问	ARN
iam:RegisterSecurityKey	按当前 MFA 设备启用状态筛选访问权限	字符串
iam:ResourceTag/${TagKey}	按附加到 IAM 实体（用户或角色）的标签筛选访问	字符串

Amazon Identity And Access Management 的操作、资源和条件键

Amazon Identity and Access Management Roles Anywhere（服务前缀:`rolesanywhere`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon Identity and Access Management Roles Anywhere 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateProfile	授予创建配置文件的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
CreateTrustAnchor	授予创建信任锚的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAttributeMapping	授予权限以从配置文件中删除映射规则	写入	profile*		
DeleteCrl	授予删除证书吊销列表 (crl) 的权限	写入	crl*		
DeleteProfile	授予删除配置文件的权限	写入	profile*		
DeleteTrustAnchor	授予删除信任锚的权限	写入	trust-anchor*		
DisableCrl	授予禁用证书吊销列表 (crl) 的权限	写入	crl*		
DisableProfile	授予禁用配置文件的权限	写入	profile*		
DisableTrustAnchor	授予禁用信任锚的权限	写入	trust-anchor*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
EnableCrl	授予启用证书吊销列表 (crl) 的权限	写入	crl*		
EnableProfile	授予启用配置文件的权限	写入	profile*		iam:PassRole
EnableTrustAnchor	授予启用信任锚的权限	写入	trust-anchor*		
GetCrl	授予权获取证书吊销列表 (crl) 的权限	读取	crl*		
GetProfile	授予获取配置文件的权限	读取	profile*		
GetSubject	授予获取主题的权限	读取	subject*		
GetTrustAnchor	授予获取信任锚的权限	读取	trust-anchor*		
ImportCrl	授予导入证书吊销列表 (crl) 的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	
ListCrls	授予列出证书吊销列表 (crl) 的权限	列表			
ListProfiles	授予列出配置文件的权限	列表			
ListSubjects	授予列出主题的权限	列表			
ListTagsForResource	授予权限以列出资源的标签	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListTrustAnchors	授予列出信任锚的权限	列表			
PutAttributeMapping	授予权限以将映射规则放入配置文件	写入	profile*		
PutNotificationSettings	授予将通知设置附加到信任锚的权限	写入	trust-anchor*		
ResetNotificationSettings	授予将自定义通知设置重置为 IAM Roles Anywhere 定义的默认状态的权限	写入	trust-anchor*		
TagResource	授予权限以标记资源	Tagging	crl		
			profile		
			subject		
			trust-anchor		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予权限以取消标记资源	标记	crl		
			profile		
			subject		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			trust-anchor		
				aws:TagKeys	
UpdateCrl	授予更新证书吊销列表 (crl) 的权限	写入	crl*		
UpdateProfile	授予更新配置文件的权限	写入	profile*		iam:PassRole
UpdateTrustAnchor	授予更新信任锚的权限	写入	trust-anchor*		

Amazon Identity and Access Management Roles Anywhere 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}

资源类型	ARN	条件键
crl	arn:${Partition}:rolesanywhere:${Region}:${Account}:crl/${CrlId}	aws:ResourceTag/${TagKey}

Amazon Identity and Access Management Roles Anywhere 的条件键

Amazon Identity and Access Management Roles Anywhere 定义了以下可以在 IAM 策略Condition元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString

Amazon Identity Store 的操作、资源和条件键

Amazon Identity Store（服务前缀:identitystore）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Identity Store 定义的操作

- Amazon Identity Store 定义的资源类型
- Amazon Identity Store 的条件键

Amazon Identity Store 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateGroup	授予在指定区域中创建群组的权限 IdentityStore	写入	Identitystore*		
CreateGroupMembership	授予在指定群组中创建成员的权限 IdentityStore	写入	Group*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			Identitystore*		
			User*		
CreateUser	授予在指定中创建用户的权限 IdentityStore	写入	Identitystore*		
DeleteGroup	授予删除指定群组的权限 IdentityStore	写入	Group*		
			Identitystore*		
DeleteGroupMembership	授予移除属于指定群组成员的权限 IdentityStore	写入	Group*		
			GroupMembership*		
			Identitystore*		
			User*		
DeleteUser	授予删除指定用户的权限 IdentityStore	写入	Identitystore*		
			User*		
DescribeGroup	授予权限以检索有关指定群组的信息 IdentityStore	读取	Group*		
			Identitystore*		
DescribeGroupMembership	授予权限以检索属于指定群组的成员的信息 IdentityStore	读取	Group*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			GroupMembership*		
			Identitystore*		
			User*		
DescribeUser	授予在指定中检索有关用户信息的权限 IdentityStore	读取	Identitystore*		
			User*		
GetGroupId	授予在指定中检索有关群组的 ID 信息的权限 IdentityStore	读取	Group*		
			Identitystore*		
GetGroupMembershipId	授予权限以检索属于指定群组的成员的 ID 信息 IdentityStore	读取	Group*		
			GroupMembership*		
			Identitystore*		
			User*		
GetUserId	授予在指定中检索有关用户的 ID 信息的权限 IdentityStore	读取	Identitystore*		
			User*		
IsMemberInGroups	授予权限以检查成员是否属于指定群组 IdentityStore	读取	AllGroupMemberships*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			Group*		
			Identitystore*		
			User*		
ListGroupMemberships	授予权限以检索属于指定群组的所有成员 IdentityStore	列表	AllGroupMemberships*		
			Group*		
			Identitystore*		
ListGroupMembershipsForMember	授予列出指定目标成员群组的权限 IdentityStore	列表	AllGroupMemberships*		
			Identitystore*		
			User*		
ListGroups	授予在指定范围内搜索群组的权限 IdentityStore	列表	AllGroups*		
			Identitystore*		
ListUsers	授予在指定区域中搜索用户的权限 IdentityStore	列表	AllUsers*		
			Identitystore*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateGroup	授予更新指定群组中群组信息的权限 IdentityStore	写入	Group*		
			Identitystore*		
UpdateUser	授予更新指定用户信息的权限 IdentityStore	写入	Identitystore*		
			User*		

Amazon Identity Store 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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/*	

资源类型	ARN	条件键
AllGroups	arn:${Partition}:identitystore:::group/*	
AllGroupMemberships	arn:${Partition}:identitystore:::membership/*	

Amazon Identity Store 的条件键

Amazon Identity Store 定义了以下可以在 IAM 策略Condition元素中使用的条件密钥。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
identitystore:UserId	按 IAM Identity Center 用户 ID 筛选访问权限	字符串

Amazon Identity Store Auth 的操作、资源和条件键

Amazon Identity Store Auth（服务前缀:identitystore-auth）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Identity Store Auth 定义的操作
- Amazon Identity Store Auth 定义的资源类型
- Amazon Identity Store Auth 的条件键

Amazon Identity Store Auth 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchDeleteSession[仅权限]	授予删除一批指定会话的权限	写入			
BatchGetSession[仅权限]	授予返回一批指定会话的会话属性的权限	读取			
ListSessions[仅权限]	授予检索指定用户的活动会话列表的权限	列表			

Amazon Identity Store Auth 定义的资源类型

Amazon Identity Store Auth 不支持在 IAM 策略声明Resource的元素中指定资源 ARN。要允许访问 Amazon Identity Store Auth，请在策略中指定 "Resource": "*"。

Amazon Identity Store Auth 的条件键

Identity Store Auth 没有可以在策略语句的 Condition 元素中使用的服务特定上下文键。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon Identity Sync 的操作、资源和条件键

Amazon Identity Sync（服务前缀:identity-sync）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

由 Amazon Identity Sync 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AllowVendedLogDeliveryForResource[仅权限]	授予权限以配置同步配置文件提供的日志传送	权限管理	SyncProfileResource*		
CreateSyncFilter	授予在同步配置文件上创建同步筛选条件的权限	写入	SyncProfileResource*		
CreateSyncProfile	授予权限以创建身份源的同步配置文件	写入			ds:AuthorizeApplication
CreateSyncTarget	授予权限以创建身份源的同步目标	写入	SyncProfileResource*		
DeleteSyncFilter	授予权限以从同步配置文件中删除同步筛选条件	写入	SyncProfileResource*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteSyncProfile	授予权限以从源中删除同步配置文件	写入	SyncProfileResource*		ds:UnauthorizeApplication
DeleteSyncTarget	授予权限以从源中删除同步目标	写入	SyncProfileResource*		
			SyncTargetResource*		
GetSyncProfile	授予权限以使用同步配置文件名称检索同步配置文件	读取	SyncProfileResource*		
GetSyncTarget	授予权限以检索同步配置文件中的同步目标	读取	SyncProfileResource*		
			SyncTargetResource*		
ListSyncFilters	授予权限以列出同步配置文件中的同步筛选条件	列表	SyncProfileResource*		
StartSync	授予权限以开启同步进程或恢复之前暂停的同步进程	写入	SyncProfileResource*		
StopSync	授予权限以阻止同步计划中任何计划内同步进程启动	写入	SyncProfileResource*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateSyncTarget	授予在同步配置文件上更新同步目标的权限	写入	SyncProfileResource*		
			SyncTargetResource*		

由 Amazon Identity Sync 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
SyncProfileResource	arn:${Partition}:identity-sync:${Region}:${Account}:profile/${SyncProfileName}	
SyncTargetResource	arn:${Partition}:identity-sync:${Region}:${Account}:target/${SyncProfileName}/${SyncTargetName}	

Amazon Identity Sync 的条件键

Identity Sync 没有可在策略语句的 Condition 元素中使用的服务特定上下文键。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon Inspector2 的操作、资源和条件键

Amazon Inspector2（服务前缀：inspector2）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon Inspector2 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateMember	授予权限以将某一账户与 Amazon Inspector 管理员账户关联	写入			
BatchGetAccountStatus	授予权限以检索有关某一账户的 Amazon Inspector 账户的信息	读取			
BatchGetCodeSnippet	授予权限以检索有关一个或多个代码漏洞调查结果的代码段信息	读取			
BatchGetFindingDetails	授予允许客户获得增强的漏洞情报详细信息以获取调查发现的权限	读取			
BatchGetFreeTrialInfo	授予权限以检索有关某一账户的 Amazon Inspector 账户的免费试用期资格	读取			
BatchGetMemberEc2DeepInspectionStatus	向委派管理员授予权限以检索成员账户的 ec2 深度检查状态	读取			
BatchUpdateMemberEc2DeepInspectionStatus	授予权限，由委派管理员为其关联的成员账户更新 ec2 深度检查状态	写入			
CancelFindingsReport	授予权限以取消调查结果报告的生成	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CancelSbomExport	授予权限以取消 SBOM 报告的生成	写入			
CreateCisScanConfiguration	授予权限以创建和定义 CIS 扫描配置的设置	写入	CIS Scan Configuration*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateFilter	授予权限以创建和定义结果筛选条件的设置	写入	Filter*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFindingsReport	授予权限以请求生成调查结果报告	写入			
CreateSbomExport	授予权限以请求生成 SBOM 报告	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteCisScanConfiguration	授予权限以删除 CIS 扫描配置	写入	CIS Scan Configuration*		
				aws:ResourceTag/${TagKey}	
DeleteFilter	授予权限以删除结果筛选条件	写入	Filter*		
DescribeOrganizationConfiguration	授予权限以检索有关 Amazon 组织的 Amazon Inspector 配置设置的信息	读取			
Disable	授予权限以禁用 Amazon Inspector 账户	写入			
DisableDelegatedAdminAccount	授予禁用账户作为 Amazon 组织委托的 Amazon Inspector 管理员账户的权限	写入			
DisassociateMember	授予 Amazon Inspector 管理员账户权限以与 Inspector 成员账户取消关联	写入			
Enable	授予权限以启用和指定新 Amazon Inspector 账户的配置设置	写入			
EnableDelegatedAdminAccount	授予允许账户作为 Amazon 组织委托的 Amazon Inspector 管理员账户的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetCisScanReport	授予权限以检索包含已完成的 CIS 扫描的信息的报告	读取			
GetCisScanResultDetails	授予权限以检索有关一个 CIS 扫描和一个目标资源的所有详细信息	列表			
GetConfiguration	授予权限以检索有关 Amazon Inspector 配置设置的信息 Amazon Web Services 账户	读取			
GetDelegatedAdminAccount	授予权限以检索有关某一账户的 Amazon Inspector 管理员账户的信息	读取			
GetEc2DeepInspectionConfiguration	授予权限以检索独立账户、委派管理员及成员账户的 ec2 深度检查状态	读取			
GetEncryptionKey	授予权限以检索有关用于加密代码片段的 KMS 密钥的信息	读取			
GetFindingsReportStatus	授予权限以检索请求的结果报告的状态	读取			
GetMember	授予权限以检索有关与 Amazon Inspector 管理员账户关联的某一账户的信息	读取			
GetSbomExport	授予权限以检索请求的 SBOM 报告	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListAccountPermissions	授予权限以检索与企业内的 Amazon Inspector 账户关联的功能配置权限	列表			
ListCisScanConfigurations	授予权限以检索有关所有 CIS 扫描配置的信息	列表			
ListCisScanResultsAggregatedByChecks	授予权限以检索有关一次 CIS 扫描的所有检查的信息	列表			
ListCisScanResultsAggregatedByTargetResource	授予权限以检索有关一次 CIS 扫描的所有资源的信息	列表			
ListCisScans	授予权限以检索已完成的 CIS 扫描的信息	列表			
ListCoverage	授予权限以检索 Amazon Inspector 可以为 Inspector 监控的资源生成的统计数据类型	列表			
ListCoverageStatistics	授予权限以检索 Amazon Inspector 监控的资源的统计数据和其他信息	列表			
ListDelegatedAdminAccounts	授予权限以检索有关 Amazon 组织委托的 Amazon Inspector 管理员账户的信息	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListFilters	授予权限以检索有关所有结果筛选条件的信息	列表			
ListFindingAggregations	授予权限以检索有关 Amazon Inspector 结果的统计数据和其他信息	列表			
ListFindings	授予权限以检索有关一个或多个结果的信息子集	列表			
ListMembers	授予权限以检索有关与 Inspector 管理员账户关联的 Amazon Inspector 成员账户的信息	列表			
ListTagsForResource	授予权限以检索 Amazon Inspector 资源的标签	读取			
ListUsageTotals	授予权限以检索账户的聚合使用情况数据	列表			
ResetEncryptionKey	授予权限以允许客户重置使用 Amazon 拥有的 KMS 密钥加密代码片段	写入			
SearchVulnerabilities	授予权限以列出特定漏洞的 Amazon Inspector 覆盖范围详细信息	读取			
SendCisSessionHealth	授予权限以发送 CIS 扫描的 CIS 运行状况	写入			
SendCisSessionTelemetry	授予权限以发送 CIS 扫描的 CIS 遥测	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StartCisSession	授予权限以开启 CIS 扫描会话	写入			
StopCisSession	授予权限以停止 CIS 扫描会话	写入			
TagResource	授予权限以为 Amazon Inspector 资源添加或更新标签	标记	CIS Scan Configuration	inspector2:CisScanConfiguration	
			Filter	inspector2:Filter	
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
UntagResource	授予从 Amazon Inspector 资源中删除标签的权限	标记	CIS Scan Configuration	inspector2:CisScanConfiguration	
			Filter	inspector2:Filter	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCisScanConfiguration	授予权限以更新 CIS 扫描配置的设置	写入	CIS Scan Configuration*		
				aws:ResourceTag/${TagKey}	
UpdateConfiguration	授予更新有关 Amazon Inspector 配置设置信息的权限 Amazon Web Services 账户	写入			
UpdateEc2DeepInspectionConfiguration	授予权限，由委派管理员、成员及独立账户更新 ec2 深度检查状态	写入			
UpdateEncryptionKey	授予权限以让用户使用 KMS 密钥加密代码片段	写入			
UpdateFilter	授予权限以更新结果筛选条件的设置	写入	Filter*		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateOrgEc2DeepInspectionConfiguration	授予权限，由委派管理员为其关联的成员账户更新 ec2 深度检查配置	写入			
UpdateOrganizationConfiguration	授予更新 Amazon 组织的 Amazon Inspector 配置设置的权限	写入			

Amazon Inspector2 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}

Amazon Inspector2 的条件键

Amazon Inspector2 定义以下可以在 IAM policy 的 `Condition` 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对来筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按附加到资源的标签键值对筛选操作	字符串
aws:TagKeys	根据在请求中是否具有标签键来筛选访问	ArrayOfString

Amazon Invoicing Service 的操作、资源和条件键

Amazon 发票服务（服务前缀:`invoicing`）提供以下特定于服务的资源、操作和条件上下文密钥，用于 IAM 权限策略。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Invoicing Service 定义的操作
- Amazon Invoicing Service 定义的资源类型
- Amazon Invoicing Service 的条件键

Amazon Invoicing Service 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchGetInvoiceProfile	授予获取组织中某个账户的发票资料详细信息的权限	读取			
CreateInvoiceUnit	授予为组织创建发票单元的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteInvoiceUnit	授予更新组织发票单位的权限	写入	invoice-unit*		
				aws:ResourceTag/${TagKey}	
GetInvoiceEmailDeliveryPreferences[仅权限]	授予获取发票电子邮件传递首选项的权限	读取			
GetInvoicePDF[仅权限]	授予获取发票 PDF 的权限	读取			
GetInvoiceUnit	授予获取组织发票单位的权限	读取	invoice-unit*		
ListInvoiceSummaries[仅权限]	授予获取您的账户或关联账户的发票摘要信息的权限	读取			
ListInvoiceUnits	授予列出组织发票单位的权限	列表			
ListTagsForResource	授予权限以列出资源的标签	读取	invoice-unit*		
				aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutInvoiceEmailDeliveryPreferences[仅权限]	授予放置发票电子邮件传递首选项的权限	写入			
TagResource	授予权限以标记资源	Tagging	invoice-unit*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	授予权限以取消标记资源	标记	invoice-unit*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateInvoiceUnit	授予更新组织发票单位的权限	写入	invoice-unit*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey}	

Amazon Invoicing Service 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
invoice-unit	arn:${Partition}:invoicing::${Account}:invoice-unit/${Identifier}	aws:ResourceTag/${TagKey}

Amazon Invoicing Service 的条件键

Amazon 开票服务定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按每个标签的允许值集筛选访问	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签值筛选访问权限	字符串
aws:TagKeys	按请求中是否具有必需标签来筛选访问	ArrayOfString

Amazon IoT Analytics 的操作、资源和条件键

Amazon IoT Analytics（服务前缀:`iotanalytics`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon IoT Analytics 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchPutMessage	将一批消息放入指定的通道	写入	channel*		
CancelPipelineReprocessing	取消指定管道的重新处理	写入	pipeline*		
CreateChannel	创建通道	写入	channel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataset	创建数据集	写入	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDatasetContent	生成指定数据集的内容（通过执行数据集操作）	写入	dataset*		
CreateDatastore	创建数据存储	写入	datastore*		
				aws:RequestTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys	
CreatePipeline	创建管道	写入	pipeline*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	删除指定的通道	写入	channel*		
DeleteDataset	删除指定的数据集	写入	dataset*		
DeleteDatasetContent	删除指定的数据集的内容	写入	dataset*		
DeleteDatastore	删除指定的数据存储	写入	datastore*		
DeletePipeline	删除指定的管道	写入	pipeline*		
DescribeChannel	描述指定的通道	读取	channel*		
DescribeDataset	描述指定的数据集	读取	dataset*		
DescribeDatastore	描述指定的数据存储	读取	datastore*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeLoggingOptions	描述账户的日志记录选项	读取			
DescribePipeline	描述指定的管道	读取	pipeline*		
GetDatasetContent	获取指定的数据集的内容	读取	dataset*		
ListChannels	列出账户的通道	列表			
ListDatasetContents	列出有关已创建数据集内容的信息	列表	dataset*		
ListDatasets	列出账户的数据集	列表			
ListDatastores	列出账户的数据存储	列表			
ListPipelines	列出账户的管道	列表			
ListTagsForResource	列出分配给资源的标签（元数据）	读取	channel		
			dataset		
			datastore		
			pipeline		
PutLoggingOptions	放入账户的日志记录选项	写入			
RunPipelineActivity	运行指定的管道活动	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
SampleChannelData	列举指定通道的数据	读取	channel*		
StartPipelineReprocessing	开始指定管道的重新处理	写入	pipeline*		
TagResource	添加或修改给定资源的标签。标签是可用于管理资源的元数据	标记	channel		
			dataset		
			datastore		
			pipeline		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	从资源中删除给定标签（元数据）	标记	channel		
			dataset		
			datastore		
			pipeline		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateChannel	更新指定的通道	写入	channel*		
UpdateDataset	更新指定的数据集	写入	dataset*		
UpdateDatastore	更新指定的数据存储	写入	datastore*		
UpdatePipeline	更新指定的管道	写入	pipeline*		

Amazon IoT Analytics 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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

资源类型	ARN	条件键
		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}

Amazon IoT Analytics 的条件键

Amazon IoT Analytics 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中传递的标签筛选访问	字符串
aws:TagKeys	根据在请求中是否具有标签键来筛选访问权限	ArrayOfString
iotanalytics:ResourceTag/${TagKey}	按附加到资源的标签键值对筛选访问权限	字符串

Amazon IoT Events 的操作、资源和条件键

Amazon IoT Events（服务前缀:iotevents）提供以下特定于服务的资源、操作和条件上下文密钥以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon IoT Events 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchAcknowledgeAlarm	授予向 Amazon IoT Events 发送一个或多个确认操作请求的权限	写入	alarmModel*		
BatchDeleteDetector	授予在 Amazon IoT Events 系统中删除探测器实例的权限	写入	detectorModel*		
BatchDisableAlarm	授予禁用一个或多个警报实例的权限	Write	alarmModel*		
BatchEnableAlarm	授予启用一个或多个警报实例的权限	写入	alarmModel*		
BatchPutMessage	授予向 Amazon IoT Events 系统发送一组消息的权限	写入	input*		
BatchResetAlarm	授予重置一个或多个警报实例的权限	Write	alarmModel*		
BatchSnoozeAlarm	授予将一个或多个警报实例更改为暂停模式的权限	写入	alarmModel*		
BatchUpdateDetector	授予在 Amazon IoT Events 系统中更新探测器实例的权限	写入	detectorModel*		
CreateAlarmModel	授予创建警报模型以监控 Amazon IoT Events 输入属性或 I Amazon oT SiteWise 资产属性的权限	写入	alarmModel*		
				aws:RequestTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys	
CreateDetectorModel	授予创建探测器模型以监控 Amazon IoT Events 输入属性的权限	写入	detectorModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInput	授予在中创建输入的权限 IotEvents	写入	input*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAlarmModel	授予删除警报模型的权限	Write	alarmModel*		
DeleteDetectorModel	授予删除探测器模型的权限	Write	detectorModel*		
DeleteInput	授予权限以删除输入	Write	input*		
DescribeAlarm	授予检索有关警报实例信息的权限	Read	alarmModel*		
DescribeAlarmModel	授予检索有关警报模型信息的权限	Read	alarmModel*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeDetector	授予检索有关探测器实例信息的权限	Read	detectorModel*		
DescribeDetectorModel	授予检索有关探测器模型信息的权限	读取	detectorModel*		
DescribeDetectorModelAnalysis	授予检索有关 detector 模型信息的权限	读取			
DescribeInput	授予检索有关输入信息的权限	读取	input*		
DescribeLoggingOptions	授予检索 Amazon IoT Events 日志选项当前设置的权限	读取			
GetDetectorModelAnalysisResults	授予权限以检索探测器模型分析结果	读取			
ListAlarmModelVersions	授予列出警报模型的所有版本的权限	List	alarmModel*		
ListAlarmModels	授予列出您创建的警报模型的权限	List			
ListAlarms	授予按 alarmModel 检索有关所有警报实例信息的权限	List	alarmModel*		
ListDetectorModelVersions	授予列出探测器模型的所有版本的权限	List	detectorModel*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListDetectorModels	授予列出您创建的探测器模型的权限	List			
ListDetectors	授予按 detectormodel 检索有关所有探测器实例信息的权限	List	detectorModel*		
ListInputRoutings	授予列出一个或多个输入路由的权限	List			
ListInputs	授予列出您创建的输入的权限	List			
ListTagsForResource	授予列出已分配给资源的标签（元数据）的权限	读取	alarmModel		
			detectorModel		
			input		
PutLoggingOptions	授予设置或更新 Amazon IoT Events 日志选项的权限	写入			
StartDetectorModelAnalysis	授予启动检测器模型分析的权限	写入			
TagResource	授予添加或修改给定资源标签的权限。标签是可用于管理资源的元数据	Tagging	alarmModel		
			detectorModel		
			input		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予从资源中删除给定标签（元数据）的权限	Tagging	alarmModel		
			detectorModel		
			input		
				aws:TagKeys	
UpdateAlarmModel	授予更新警报模型的权限	Write	alarmModel*		
UpdateDetectorModel	授予更新探测器模型的权限	Write	detectorModel*		
UpdateInput	授予权限以更新输入	Write	input*		
UpdateInputRouting	授予更新输入路由的权限	Write	input*		

Amazon IoT Events 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}

Amazon IoT Events 的条件键

Amazon IoT Events 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中的标签键值对筛选访问	字符串
aws:ResourceTag/${TagKey}	按附加到资源的标签筛选访问	字符串
aws:TagKeys	按请求中的标签键筛选操作	ArrayOfString
iotevents:keyValue	按消息的 instanceId（键值）筛选访问权限	字符串

Amazon IoT Greengrass 的操作、资源和条件键

Amazon IoT Greengrass（服务前缀greengrass:）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon IoT Greengrass 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateRoleToGroup	授予权限以将角色与组相关联。该角色的权限必须允许 Greengrass 核心 Lambda 函数和连接器在其他服务中执行操作 Amazon	写入	group*		
AssociateServiceRoleToAccount	授予将角色与您的账户关联的权限。 Amazon IoT Greengrass 使用此角色访问您的 Lambda 函数和物联网资源 Amazon	权限管理			
CreateConnectorDefinition	授予权限以创建连接器定义	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnectorDefinitionVersion	授予权限以创建现有连接器定义的版本	Write	connectorDefinition*		
CreateCoreDefinition	授予权限以创建核心定义	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCoreDefinitionVersion	授予权限以创建现有核心定义的版本。每个 Greengrass 组	Write	coreDefinition*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
	必须恰好包含 1 个 Greengrass 核心				
CreateDeployment	授予创建部署的权限	Write	group*		
CreateDeviceDefinition	授予权限以创建设备定义	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeviceDefinitionVersion	授予权限以创建现有设备定义的版本	Write	deviceDefinition*		
CreateFunctionDefinition	授予权限以创建在组中使用的 Lambda 函数定义，其中包含 Lambda 函数及其配置列表	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFunctionDefinitionVersion	授予权限以创建现有 Lambda 函数定义的版本	写入	functionDefinition*		
CreateGroup	授予权限以创建组	写入		aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateGroupCertificateAuthority	授予权限以创建组的 CA 或轮换现有的 CA	Write	group*		
CreateGroupVersion	授予权限以创建已定义的组的版本	Write	group*		
CreateLoggerDefinition	授予权限以创建记录器定义	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLoggerDefinitionVersion	授予权限以创建现有记录器定义的版本	Write	loggerDefinition*		
CreateResourceDefinition	授予权限以创建资源定义，其中包含要在组中使用的资源列表	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateResourceDefinitionVersion	授予权限以创建现有资源定义的版本	写入	resourceDefinition*		
CreateSoftwareUpdateJob	授予创建 Amazon 物联网任务的权限，该任务将触发您的 Greengrass 内核更新正在运行的软件	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateSubscriptionDefinition	授予权限以创建订阅定义	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscriptionDefinitionVersion	授予权限以创建现有订阅定义的版本	Write	subscriptionDefinition*		
DeleteConnectorDefinition	授予权限以删除连接器定义	Write	connectorDefinition*		
DeleteCoreDefinition	授予权限以删除核心定义。删除当前在部署中使用的定义将会影响将来的部署	Write	coreDefinition*		
DeleteDeviceDefinition	授予权限以删除设备定义。删除当前在部署中使用的定义将会影响将来的部署	Write	deviceDefinition*		
DeleteFunctionDefinition	授予权限以删除 Lambda 函数定义。删除当前在部署中使用的定义将会影响将来的部署	Write	functionDefinition*		
DeleteGroup	授予权限以删除当前在部署中未使用的组	Write	group*		
DeleteLoggerDefinition	授予权限以删除记录器定义。删除当前在部署中使用的定义将会影响将来的部署	Write	loggerDefinition*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteResourceDefinition	授予权限以删除资源定义	Write	resourceDefinition*		
DeleteSubscriptionDefinition	授予权限以删除订阅定义。删除当前在部署中使用的定义将会影响将来的部署	Write	subscriptionDefinition*		
DisassociateRoleFromGroup	授予权限以将角色与组取消关联	Write	group*		
DisassociateServiceRoleFromAccount	授予权限以将服务角色与账户取消关联。如果没有服务角色，部署将不起作用	Write			
Discover	授予权限以检索连接到 Greengrass 核心所需的信息	Read	thing*		
GetAssociatedRole	授予权限以检索与组关联的角色	Read	group*		
GetBulkDeploymentStatus	授予权限以返回批量部署的状态	Read	bulkDeployment*		
GetConnectivityInfo	授予权限以检索核心的连接信息	Read	connectivityInfo*		
GetConnectorDefinition	授予权限以检索有关连接器定义的信息	Read	connectorDefinition*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetConnectorDefinitionVersion	授予权限以检索有关连接器定义版本的信息	Read	connectorDefinition*		
			connectorDefinitionVersion*		
GetCoreDefinition	授予权限以检索有关核心定义的信息	Read	coreDefinition*		
GetCoreDefinitionVersion	授予权限以检索有关核心定义版本的信息	Read	coreDefinition*		
			coreDefinitionVersion*		
GetDeploymentStatus	授予权限以返回部署的状态	Read	deployment*		
			group*		
GetDeviceDefinition	授予权限以检索有关设备定义的信息	Read	deviceDefinition*		
GetDeviceDefinitionVersion	授予权限以检索有关设备定义版本的信息	Read	deviceDefinition*		
			deviceDefinitionVersion*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetFunctionDefinition	授予权限以检索有关 Lambda 函数定义的信息，例如其创建时间和最新版本	Read	functionDefinition*		
GetFunctionDefinitionVersion	授予权限以检索有关 Lambda 函数定义版本的信息，例如在版本中包含的 Lambda 函数及其配置	Read	functionDefinition*		
			functionDefinitionVersion*		
GetGroup	授予权限以检索有关组的信息	Read	group*		
GetGroupCertificateAuthority	授予权限以返回与组关联的 CA 的公有密钥	Read	certificateAuthority*		
			group*		
GetGroupCertificateConfiguration	授予权限以检索组使用的 CA 的当前配置	Read	group*		
GetGroupVersion	授予权限以检索有关组版本的信息	Read	group*		
			groupVersion*		
GetLoggerDefinition	授予权限以检索有关记录器定义的信息	Read	loggerDefinition*		
GetLoggerDefinitionVersion	授予权限以检索有关记录器定义版本的信息	Read	loggerDefinition*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			loggerDefinitionVersion*		
GetResourceDefinition	授予权限以检索有关资源定义的信息，例如其创建时间和最新版本	Read	resourceDefinition*		
GetResourceDefinitionVersion	授予权限以检索有关资源定义版本的信息，例如在版本中包含的资源	Read	resourceDefinition*		
			resourceDefinitionVersion*		
GetServiceRoleForAccount	授予权限以检索附加到账户的服务角色	Read			
GetSubscriptionDefinition	授予权限以检索有关订阅定义的信息	Read	subscriptionDefinition*		
GetSubscriptionDefinitionVersion	授予权限以检索有关订阅定义版本的信息	Read	subscriptionDefinition*		
			subscriptionDefinitionVersion*		
GetThingRuntimeConfiguration	授予权限以检索事物的运行时配置	Read	thingRuntimeConfig*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListBulkDeploymentDetailedReports	授予权限以检索已在批量部署操作中启动的部署及其当前部署状态的分页列表	Read	bulkDeployment*		
ListBulkDeployments	授予权限以检索批量部署列表	List			
ListConnectorDefinitionVersions	授予权限以列出连接器定义版本	List	connectorDefinition*		
ListConnectorDefinitions	授予权限以检索连接器定义列表	List			
ListCoreDefinitionVersions	授予权限以列出核心定义版本	List	coreDefinition*		
ListCoreDefinitions	授予权限以检索核心定义列表	List			
ListDeployments	授予权限以检索组的所有部署的列表	List	group*		
ListDeviceDefinitionVersions	授予权限以列出设备定义版本	List	deviceDefinition*		
ListDeviceDefinitions	授予权限以检索设备定义列表	List			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListFunctionDefinitionVersions	授予权限以列出 Lambda 函数定义版本	List	functionDefinition*		
ListFunctionDefinitions	授予权限以检索 Lambda 函数定义列表	列表			
ListGroupCertificateAuthorities	授予检索群组当前列表 CAs 的权限	列表	group*		
ListGroupVersions	授予权限以列出组版本	List	group*		
ListGroups	授予权限以检索组列表	List			
ListLoggerDefinitionVersions	授予权限以列出记录器定义版本	List	loggerDefinition*		
ListLoggerDefinitions	授予权限以检索记录器定义列表	List			
ListResourceDefinitionVersions	授予权限以列出资源定义版本	List	resourceDefinition*		
ListResourceDefinitions	授予权限以检索资源定义列表	List			
ListSubscriptionDefinitionVersions	授予权限以列出订阅定义版本	List	subscriptionDefinition*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListSubscriptionDefinitions	授予权限以检索订阅定义列表	List			
ListTagsForResource	授予列出资源标签的权限	Read	bulkDeployment		
			connectorDefinition		
			coreDefinition		
			deviceDefinition		
			functionDefinition		
			group		
			loggerDefinition		
			resourceDefinition		
			subscriptionDefinition		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
ResetDeployments	授予权限以重置组的部署	Write	group*		
StartBulkDeployment	授予权限以在一个操作中部署多个组	Write		aws:RequestTag/${TagKey} aws:TagKeys	
StopBulkDeployment	授予权限以停止执行批量部署	Write	bulkDeployment*		
TagResource	授予权限以将标签添加到资源中	Tagging	bulkDeployment		
			connectorDefinition		
			coreDefinition		
			deviceDefinition		
			functionDefinition		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			group		
			loggerDefinition		
			resourceDefinition		
			subscriptionDefinition		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予权限以从资源中删除标签	Tagging	bulkDeployment		
			connectorDefinition		
			coreDefinition		
			deviceDefinition		
			functionDefinition		
			group		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			loggerDefinition		
			resourceDefinition		
			subscriptionDefinition		
				aws:TagKeys	
UpdateConnectivityInfo	授予权限以更新 Greengrass 核心的连接信息。属于具有该核心的组的任何设备都会收到该信息，以便查找该核心的位置并连接到该核心	Write	connectivityInfo*		
UpdateConnectorDefinition	授予权限以更新连接器定义	Write	connectorDefinition*		
UpdateCoreDefinition	授予权限以更新核心定义	Write	coreDefinition*		
UpdateDeviceDefinition	授予权限以更新设备定义	Write	deviceDefinition*		
UpdateFunctionDefinition	授予权限以更新 Lambda 函数定义	Write	functionDefinition*		
UpdateGroup	授予权限以更新组	Write	group*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateGroupCertificateConfiguration	授予权限以更新组的证书到期时间	Write	group*		
UpdateLoggerDefinition	授予权限以更新记录器定义	Write	loggerDefinition*		
UpdateResourceDefinition	授予权限以更新资源定义	Write	resourceDefinition*		
UpdateSubscriptionDefinition	授予权限以更新订阅定义	Write	subscriptionDefinition*		
UpdateThingRuntimeConfiguration	授予权限以更新事物的运行时配置	Write	thingRuntimeConfig*		

Amazon IoT Greengrass 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
connectivityInfo	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/things/${ThingName}/connectivityInfo	

资源类型	ARN	条件键
certificateAuthority	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}/certificateauthorities/${CertificateAuthorityId}	
deployment	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}/deployments/${DeploymentId}	
bulkDeployment	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/bulk/deployments/${BulkDeploymentId}	aws:ResourceTag/${TagKey}
group	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}	aws:ResourceTag/${TagKey}
groupVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}/versions/${VersionId}	
coreDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/cores/${CoreDefinitionId}	aws:ResourceTag/${TagKey}
coreDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/cores/${CoreDefinitionId}/versions/${VersionId}	
deviceDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/devices/${DeviceDefinitionId}	aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
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}
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}

资源类型	ARN	条件键
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	

Amazon IoT Greengrass 的条件键

Amazon IoT Greengrass 定义了以下条件键，这些条件键可用于 IAM 策略Condition的元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按每个必需标签的允许值集筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签值筛选访问权限	字符串

条件键	描述	类型
aws:TagKeys	按请求中是否具有必需标签来筛选访问	ArrayOfString

Amazon IoT Greengrass V2 的操作、资源和条件键

Amazon IoT Greengrass V2（服务前缀greengrass:）提供了以下特定于服务的资源、操作和条件上下文密钥，用于 IAM 权限策略。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon IoT Greengrass V2 定义的操作
- Amazon IoT Greengrass V2 定义的资源类型
- Amazon IoT Greengrass V2 的条件键

Amazon IoT Greengrass V2 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateServiceRoleToAccount	授予将角色与您的账户关联的权限。 Amazon IoT Greengrass 使用此角色访问您的 Lambda 函数和物联网资源 Amazon	权限管理			iam:PassRole
BatchAssociateClientDeviceWithCoreDevice	授予权限以将客户端设备列表与核心设备关联	写入	coreDevice*		
BatchDisassociateClientDeviceFromCoreDevice	授予权限以取消客户端设备列表与核心设备的关联	写入	coreDevice*		
CancelDeployment	授予取消部署的权限	Write	deployment*		iot:CancelJob iot:DeleteThingShadow

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
					iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow iot:UpdateJob iot:UpdateThingShadow
CreateComponentVersion	授予创建组件的权限	Write	component *		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateDeployment	授予创建部署的权限	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	授予删除组件的权限	写入	componentVersion*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteCoreDevice	授予删除 Amazon 物联网 Greengrass 核心设备的权限，这是物联网的东西。 Amazon 此操作将从核心设备列表中删除该核心设备。此操作不会删除 Amazon 物联网的东西	写入	coreDevice*		iot:DescribeJobExecution
DeleteDeployment	授予权限以删除部署。要删除活动部署，需要先将其取消	写入	deployment*		iot:DeleteJob
DescribeComponent	授予检索组件版本元数据的权限	读取	componentVersion*		
DisassociateServiceRoleFromAccount	授予权限以将服务角色与账户取消关联。如果没有服务角色，部署将不起作用	写入			
GetComponent	授予获取组件版本配方的权限	Read	componentVersion*		
GetComponentVersionArtifact	授予获取预签名 URL 以下载公有组件的权限	读取	componentVersion*		
GetConnectivityInfo	授予权限以检索 Greengrass 核心设备的连接信息	读取	connectivityInfo*		iot:GetThingShadow
GetCoreDevice	授予检索 Amazon 物联网 Greengrass 核心设备元数据的权限	读取	coreDevice*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetDeployment	授予获取部署的权限	读取	deployment*		iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow
GetServiceRoleForAccount	授予权限以检索附加到账户的服务角色	读取			
ListClientDevicesAssociatedWithCoreDevice	授予检索与 Amazon 物联网 Greengrass 核心设备关联的分页客户端设备列表的权限	列表	coreDevice*		
ListComponentVersions	授予检索组件所有版本的分页列表的权限	List	component*		
ListComponents	授予检索组件摘要的分页列表的权限	列表			
ListCoreDevices	授予检索 Amazon 物联网 Greengrass 核心设备分页列表的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListDeployments	授予检索部署分页列表的权限	列表			iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow
ListEffectiveDeployments	允许检索 IoT Greengrass 发送到物联网 Amazon Greengrass 核心设备的分页部署任务列表 Amazon	列表	coreDevice*		iot:DescribeJob iot:DescribeJobExecution iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow
ListInstalledComponents	授予检索 Amazon IoT Greengrass 核心设备运行的组件的分页列表的权限	列表	coreDevice*		
ListTagsForResource	授予列出资源标签的权限	读取	component		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			componentVersion		
			coreDevice		
			deployment		
				aws:RequestTag/${TagKey} aws:TagKeys	
ResolveComponentCandidates	授予列出符合部署组件、版本和平台要求的组件的权限	List	componentVersion*		
TagResource	授予权限以将标签添加到资源中	Tagging	component		
			componentVersion		
			coreDevice		
			deployment		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予权限以从资源中删除标签	Tagging	component		
			componentVersion		
			coreDevice		
			deployment		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateConnectivityInfo	授予权限以更新 Greengrass 核心的连接信息。属于具有该核心的组的任何设备都会收到该信息，以便查找该核心的位置并连接到该核心	写入	connectivityInfo*		iot:GetThingShadow iot:UpdateThingShadow

Amazon IoT Greengrass V2 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}

Amazon IoT Greengrass V2 的条件键

Amazon IoT Greengrass V2 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	通过检查请求中包含的标签键值对筛选访问权限	字符串
aws:ResourceTag/${TagKey}	通过检查与特定资源关联的标签键/值对筛选访问权限	字符串
aws:TagKeys	通过检查请求中传递的标签键筛选访问权限	ArrayOfString

Amazon 物联网任务的操作、资源和条件键 DataPlane

Amazon IoT 任务 DataPlane（服务前缀:`iotjobsdata`）提供以下特定于服务的资源、操作和条件上下文密钥，以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon 物联网任务定义的操作 DataPlane
- Amazon 物联网任务定义的资源类型 DataPlane
- Amazon 物联网任务的条件密钥 DataPlane

Amazon 物联网任务定义的操作 DataPlane

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，

以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeJobExecution	授予描述作业执行的权限	读取	thing*		
				iot:JobId	
GetPendingJobExecutions	授予获取未处于终端状态的事物的所有作业列表的权限	读取	thing*		
StartNextPendingJobExecution	授予权限，以为事物获取和启动下一个待处理作业执行	写入	thing*		
UpdateJobExecution	授予更新作业执行的权限	写入	thing*		
				iot:JobId	

Amazon 物联网任务定义的资源类型 DataPlane

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
thing	arn:${Partition}:iot:${Region}:${Account}:thing/${ThingName}	

Amazon 物联网任务的条件密钥 DataPlane

Amazon IoT Jobs DataPlane 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
iot:JobId	按 jobid 筛选 iotjobsdata: 和 iotjobsdata 的访问权限：DescribeJobExecution UpdateJobExecution APIs	字符串

Amazon 物联网的操作、资源和条件键 SiteWise

Amazon IoT SiteWise （服务前缀:iotsitewise）提供以下特定于服务的资源、操作和条件上下文密钥以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon 物联网定义的操作 SiteWise
- Amazon 物联网定义的资源类型 SiteWise
- Amazon 物联网的条件密钥 SiteWise

Amazon 物联网定义的操作 SiteWise

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateAssets	授予权限以通过层次结构将子资产与父资产关联	写入	asset*		
AssociateTimeSerie	授予权限以将时间序列与资产属性关联起来	写入	asset*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
sToAssetProperty			time-series*		
BatchAssociateProjectAssets	授予权限以将资产关联到项目	Write	project*		
BatchDisassociateProjectAssets	授予权限以取消资产与项目的关联	写入	project*		
BatchGetAssetPropertyAggregates	授予权限以检索多个资产属性的计算聚合	读取	asset		
			time-series		
BatchGetAssetPropertyValue	授予权限以检索多个资产属性的最新值	读取	asset		
			time-series		
BatchGetAssetPropertyValueHistory	授予权限以检索多个资产属性的值历史记录	读取	asset		
			time-series		
BatchPutAssetPropertyValue	授予权限以便为资产属性放置属性值	Write	asset		
			time-series		
CreateAccessPolicy	授予权限以便为门户或项目创建访问策略	Write	portal		
			project		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAsset	授予权限以从资产模型创建资产	Write	asset-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssetModel	授予权限以创建资产模型	写入		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssetModelCompositeModel	授予在资产模型中创建资产模型复合模型的权限	写入	asset-model*		
CreateBulkImportJob	授予权限以创建批量导入任务	写入			
CreateDashboard	授予权限以在项目中创建控制面板	写入	project*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataset	授予创建数据集的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	
CreateGateway	授予权限以创建网关	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePortal	授予权限以创建门户	Write		aws:RequestTag/${TagKey} aws:TagKeys	sso:CreateManagedApplicationInstance sso:DescribeRegisteredRegions
CreateProject	授予权限以在门户中创建项目	Write	portal*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessPolicy	授予权限以删除访问策略	Write	access-policy*		
DeleteAsset	授予权限以删除资产	Write	asset*		
DeleteAssetModel	授予权限以删除资产模型	写入	asset-model*		
DeleteAssetModelCompositeModel	授予删除资产模型复合模型的权限	写入	asset-model*		
DeleteDashboard	授予权限以删除控制面板	写入	dashboard*		
DeleteDataset	授予删除数据库的权限	写入	dataset*		
DeleteGateway	授予权限以删除网关	Write	gateway*		
DeletePortal	授予权限以删除门户	Write	portal*		sso:DeleteManagedApplicationInstance

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteProject	授予权限以删除项目	写入	project*		
DeleteTimeSeries	授予删除时间序列的权限	写入	asset		
			time-series		
DescribeAccessPolicy	授予权限以描述访问策略	读取	access-policy*		
DescribeAction	授予描述操作的权限	读取	asset		
DescribeAsset	授予权限以描述资产	读取	asset*		
DescribeAssetCompositeModel	授予描述资产复合模型的权限	读取	asset*		
DescribeAssetModel	授予权限以描述资产模型	读取	asset-model*		
DescribeAssetModelCompositeModel	授予描述资产模型复合模型的权限	读取	asset-model*		
DescribeAssetProperty	授予权限以描述资产属性	读取	asset*		
DescribeBulkImportJob	授予权限以描述批量导入任务	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeDashboard	授予权限以描述控制面板	读取	dashboard*		
DescribeDataset	授予描述数据集的权限	读取	dataset*		
DescribeDefaultEncryptionConfiguration	授予描述默认加密配置的权限 Amazon Web Services 账户	读取			
DescribeGateway	授予权限以描述网关	Read	gateway*		
DescribeGatewayCapabilityConfiguration	授予权限以描述网关的功能配置	读取	gateway*		
DescribeLoggingOptions	授予描述日志选项的权限 Amazon Web Services 账户	读取			
DescribePortal	授予权限以描述门户	Read	portal*		
DescribeProject	授予权限以描述项目	读取	project*		
DescribeStorageConfiguration	授予描述存储配置的权限 Amazon Web Services 账户	读取			
DescribeTimeSeries	授予描述时间序列的权限	读取	asset		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			time-series		
				aws:RequestTag/${TagKey} aws:TagKeys	
DisassociateAssets	授予权限以按层次结构取消子资产与父资产的关联	写入	asset*		
DisassociateTimeSeriesFromAssetProperty	授予权限以取消时间序列与资产属性的关联	写入	asset*		
			time-series*		
EnableSiteWiseIntegration[仅权限]	授予允许 IoT 与其他服务 SiteWise 集成的权限	写入			
ExecuteAction	授予执行操作的权限	写入	asset		
ExecuteQuery	授予权限以执行查询	读取			
GetAssetPropertyAggregates	授予权限以检索资产属性的计算聚合	Read	asset		
			time-series		
GetAssetPropertyValue	授予权限以检索资产属性的最新值	Read	asset		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			time-series		
GetAssetPropertyValueHistory	授予权限以检索资产属性的值历史记录	读取	asset		
			time-series		
GetInterpolatedAssetPropertyValues	授予权限以检索资产属性的内插值	读取	asset		
			time-series		
InvokeAssistant	授予调用助手的权限	读取			
ListAccessPolicies	授予权限以列出身份或资源的所有访问策略	列表	portal		
			project		
ListActions	授予列出所有操作的权限	列表	asset		
ListAssetModelCompositeModels	授予列出所有资产模型复合模型的权限	列表	asset-model*		
ListAssetModelProperties	授予列出所有资产模型属性的权限	列表	asset-model*		
ListAssetModels	授予权限以列出所有资产模型	列表			
ListAssetProperties	授予列出所有资产属性的权限	列表	asset*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListAssetRelationships	授予列出资产的资产关系图的权限	List	asset*		
ListAssets	授予权限以列出所有资产	列表	asset-model		
ListAssociatedAssets	授予权限以通过层次结构列出与资产关联的所有资产	列表	asset*		
ListBulkImportJobs	授予权限以列出批量导入任务	列表			
ListCompositionRelationships	授予列出所有资产模型合成关系的权限	列表	asset-model*		
ListDashboards	授予权限以列出项目中的所有控制面板	列表	project*		
ListDatasets	授予列出所有数据集的权限	列表			
ListGateways	授予权限以列出所有网关	List			
ListPortals	授予权限以列出所有门户	List			
ListProjectAssets	授予权限以列出与项目关联的所有资产	List	project*		
ListProjects	授予权限以列出门户中的所有项目	List	portal*		
ListTagsForResource	授予权限以列出资源的所有标签	读取	access-policy		
			asset		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			asset-model		
			dashboard		
			dataset		
			gateway		
			portal		
			project		
			time-series		
				aws:ResourceTag/${TagKey}	
ListTimeSeries	授予列出时间序列的权限	列表	asset		
PutDefaultEncryptionConfiguration	授予设置默认加密配置的权限 Amazon Web Services 账户	写入			
PutLoggingOptions	授予为设置日志记录选项的权限 Amazon Web Services 账户	写入			
PutStorageConfiguration	授予为配置存储设置的权限 Amazon Web Services 账户	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
TagResource	授予权限以标记资源	Tagging	access-policy		
			asset		
			asset-model		
			dashboard		
			dataset		
			gateway		
			portal		
			project		
			time-series		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	授予权限以取消标记资源	Tagging	access-policy		
			asset		
			asset-model		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			dashboard		
			dataset		
			gateway		
			portal		
			project		
			time-series		
				aws:TagKeys	
UpdateAccessPolicy	授予权限以更新访问策略	Write	access-policy*		
UpdateAsset	授予权限以更新资产	Write	asset*		
UpdateAssetModel	授予权限以更新资产模型	写入	asset-model*		
UpdateAssetModelCompositeModel	授予更新资产模型复合模型的权限	写入	asset-model*		
UpdateAssetModelPropertyRouting[仅权限]	授予更新 AssetModel 属性路由的权限	写入	asset-model*		
UpdateAssetProperty	授予权限以更新资产属性	Write	asset*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateDashboard	授予权限以更新控制面板	写入	dashboard*		
UpdateDataset	授予更新数据集的权限	写入	dataset*		
UpdateGateway	授予权限以更新网关	Write	gateway*		
UpdateGatewayCapabilityConfiguration	授予权限以更新网关的功能配置	Write	gateway*		
UpdatePortal	授予权限以更新门户	Write	portal*		
UpdateProject	授予权限以更新项目	写入	project*		

Amazon 物联网定义的资源类型 SiteWise

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
asset	arn:${Partition}:iotsitewise:${Region}:${Account}:asset/${AssetId}	aws:ResourceTag/${TagKey}
asset-model	arn:${Partition}:iotsitewise:${Region}:${Account}:asset-model/${AssetModelId}	aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
time-series	arn:${Partition}:iotsitewise:${Region}:${Account}:time-series/${TimeSeriesId}	aws:ResourceTag/${TagKey}
gateway	arn:${Partition}:iotsitewise:${Region}:${Account}:gateway/${GatewayId}	aws:ResourceTag/${TagKey}
portal	arn:${Partition}:iotsitewise:${Region}:${Account}:portal/${PortalId}	aws:ResourceTag/${TagKey}
project	arn:${Partition}:iotsitewise:${Region}:${Account}:project/${ProjectId}	aws:ResourceTag/${TagKey}
dashboard	arn:${Partition}:iotsitewise:${Region}:${Account}:dashboard/${DashboardId}	aws:ResourceTag/${TagKey}
access-policy	arn:${Partition}:iotsitewise:${Region}:${Account}:access-policy/${AccessPolicyId}	aws:ResourceTag/${TagKey}
dataset	arn:${Partition}:iotsitewise:${Region}:${Account}:dataset/${DatasetId}	aws:ResourceTag/${TagKey}

Amazon 物联网的条件密钥 SiteWise

Amazon IoT SiteWise 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中的标签键值对筛选访问	字符串

条件键	描述	类型
aws:ResourceTag/${TagKey}	按附加到资源的标签筛选访问	字符串
aws:TagKeys	按请求中的标签键筛选访问权限	ArrayOfString
iotsitewise:assetHierarchyPath	按资产层次结构路径筛选访问权限，该路径是资产层次结构 IDs 中的资产字符串，每个路径由正斜杠隔开	字符串
iotsitewise:childAssetId	按与父资产关联的子资产的 ID 筛选访问权限	字符串
iotsitewise:group	按 Amazon 单点登录群组的 ID 筛选访问权限	字符串
iotsitewise:iam	按 Amazon IAM 身份的 ID 筛选访问权限	字符串
iotsitewise:isAssociatedWithAssetProperty	按与资产属性关联或不关联的数据流筛选访问权限	字符串
iotsitewise:portal	按门户 ID 筛选访问	字符串
iotsitewise:project	按项目 ID 筛选访问	字符串
iotsitewise:propertyAlias	按属性别名筛选访问权限	字符串
iotsitewise:propertyId	按资产属性的 ID 筛选访问	字符串
iotsitewise:user	按 Amazon 单点登录用户的 ID 筛选访问权限	字符串

Amazon 物联网的操作、资源和条件键 TwinMaker

Amazon IoT TwinMaker （服务前缀:`iottwinmaker`）提供以下特定于服务的资源、操作和条件上下文密钥以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon 物联网定义的操作 TwinMaker

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchPutPropertyValues	授予为多个时间序列属性设置值的权限	写入	workspace*		iottwinmaker:GetComponentType iottwinmaker:GetEntity iottwinmaker:GetWorkspace
			entity		
CancelMetadataTransferJob	授予取消元数据传输作业的权限	写入	metadataTransferJob*		
CreateComponentType	授予创建 componentType 的权限	写入	workspace*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEntity	授予创建实体的权限	写入	workspace*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMetadataTransferJob	授予创建元数据传输作业的权限	写入			
CreateScene	授予创建场景的权限	写入	workspace*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSyncJob	授予权限以创建同步作业	写入	workspace*		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateWorkspace	授予创建工作区的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteComponentType	授予删除 componentType 的权限	写入	componentType*		
			workspace*		
DeleteEntity	授予删除实体的权限	写入	entity*		
			workspace*		
DeleteScene	授予删除场景的权限	写入	scene*		
			workspace*		
DeleteSyncJob	授予权限以删除同步作业	写入	syncJob*		
			workspace*		
DeleteWorkspace	授予删除工作区的权限	写入	workspace*		
ExecuteQuery	授予权限以执行查询	读取	workspace*		
GetComponentType	授予获取 componentType 的权限	读取	componentType*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			workspace*		
GetEntity	授予获取实体的权限	读取	entity*		
			workspace*		
GetMetadataTransferJob	授予获取元数据传输作业的权限	读取	metadataTransferJob*		
GetPricingPlan	授予权限以获取定价计划	读取			
GetPropertyValue	授予权限以检索属性值	读取	workspace*		iottwinmaker:GetComponentType iottwinmaker:GetEntity iottwinmaker:GetWorkspace
			componentType		
			entity		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetPropertyValueHistory	授予权限以检索时间序列值历史记录	读取	workspace*		iottwinmaker:GetComponentType iottwinmaker:GetEntity iottwinmaker:GetWorkspace
			componentType		
			entity		
GetScene	授予获取场景的权限	读取	scene*		
			workspace*		
GetSyncJob	授予权限以获取同步作业	读取	syncJob*		
			workspace*		
GetWorkspace	授予获取工作区的权限	读取	workspace*		
ListComponentTypes	授予列出工作区中所有 componentType 的权限	列表	workspace*		
ListComponents	授予列出附加到实体的组件的权限	列表	entity*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			workspace*		
ListEntities	授予列出工作区中所有实体的权限	列表	workspace*		
ListMetadataTransferJobs	授予列出所有元数据传输作业的权限	列表			
ListProperties	授予列出实体组件的属性的权限	列表	entity*		
			workspace*		
ListScenes	授予列出工作区中所有场景的权限	列表	workspace*		
ListSyncJobs	授予权限以列出工作空间中的所有同步作业	列表	workspace*		
ListSyncResources	授予权限以列出同步作业的所有同步资源	列表	syncJob*		
			workspace*		
ListTagsForResource	授予权限以列出资源的所有标签	列表	componentType		
			entity		
			scene		
			syncJob		
			workspace		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey}	
ListWorkspaces	授予权限以列出所有工作区	列表			
TagResource	授予权限以标记资源	Tagging	componentType		
			entity		
			scene		
			syncJob		
			workspace		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予权限以取消标记资源	标记	componentType		
			entity		
			scene		
			syncJob		
			workspace		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys	
UpdateComponentType	授予更新 componentType 的权限	写入	componentType*		
			workspace*		
UpdateEntity	授予权限以更新实体	写入	entity*		
			workspace*		
UpdatePricingPlan	授予权限以更新定价计划	写入			
UpdateScene	授予更新场景的权限	写入	scene*		
			workspace*		
UpdateWorkspace	授予权限以更新工作区	写入	workspace*		

Amazon 物联网定义的资源类型 TwinMaker

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}	

Amazon 物联网的条件密钥 TwinMaker

Amazon IoT TwinMaker 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中的标签键值对筛选访问	字符串
aws:ResourceTag/${TagKey}	按附加到资源的标签筛选访问	字符串
aws:TagKeys	按请求中的标签键筛选访问权限	ArrayOfString
iottwinmaker:destinationType	按元数据传输作业的目的地类型筛选访问权限	ArrayOfString
iottwinmaker:linkedServices	按与服务关联的工作区筛选访问权限	ArrayOfString
iottwinmaker:sourceType	按元数据传输作业的源类型筛选访问权限	ArrayOfString

Amazon Kinesis Analytics 的操作、资源和条件键

Amazon Kinesis Analytics（服务前缀：`kinesisanalytics`）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Kinesis Analytics 定义的操作
- Amazon Kinesis Analytics 定义的资源类型
- Amazon Kinesis Analytics 的条件键

Amazon Kinesis Analytics 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddApplicationInput	授予权限以向应用程序添加输入	写入	application*		
AddApplicationOutput	授予权限以向应用程序添加输出	Write	application*		
AddApplicationReferenceDataSource	授予权限以向应用程序添加引用数据源	写入	application*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateApplication	授予创建应用程序的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	授予权限以删除应用程序	写入	application*		
DeleteApplicationOutput	授予权限以删除应用程序的指定输出	Write	application*		
DeleteApplicationReferenceDataSource	授予权限以删除应用程序的指定引用数据源	写入	application*		
DescribeApplication	授予权限以描述指定应用程序	读取	application*		
DiscoverInputSchema	授予权限以发现应用程序输入架构	读取			
GetApplicationState[仅权限]	向 Kinesis Data Analytics 控制台授予权限，以显示 Kinesis Data Analytics SQL 运行时应用程序的流式处理结果	读取	application*		
ListApplications	授予权限以列出账户应用程序	List			
ListTagsForResource	授予权限以获取与应用程序关联的标签	Read	application*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StartApplication	授予权限以启动应用程序	Write	application*		
StopApplication	授予权限以停止应用程序	Write	application*		
TagResource	授予权限以向应用程序添加标签	Tagging	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予权限以从应用程序中删除指定标签	Tagging	application*		
				aws:TagKeys	
UpdateApplication	授予权限以更新应用程序	写入	application*		

Amazon Kinesis Analytics 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
application	arn:${Partition}:kinesisanalytics:${Region}:${Account}:application/${ApplicationName}	aws:ResourceTag/${TagKey}

Amazon Kinesis Analytics 的条件键

Amazon Kinesis Analytics 定义以下可以在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按每个标签的值集筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签值筛选访问权限	字符串
aws:TagKeys	按请求中是否有必需标签键来筛选访问权限	ArrayOfString

Amazon Kinesis Analytics V2 的操作、资源和条件键

Amazon Kinesis Analytics V2（服务前缀：kinesisanalytics）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Kinesis Analytics V2 定义的操作
- Amazon Kinesis Analytics V2 定义的资源类型
- Amazon Kinesis Analytics V2 的条件键

Amazon Kinesis Analytics V2 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddApplicationCloudWatchLoggingOption	授予权限以向应用程序添加 cloudwatch 日志记录选项	Write	application*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddApplicationInput	授予权限以向应用程序添加输入	Write	application*		
AddApplicationInputProcessingConfiguration	授予权限以向应用程序添加输入处理配置	Write	application*		
AddApplicationOutput	授予权限以向应用程序添加输出	Write	application*		
AddApplicationReferenceDataSource	授予权限以向应用程序添加引用数据源	Write	application*		
AddApplicationVpcConfiguration	授予权限以向应用程序添加 VPC 配置	Write	application*		
CreateApplication	授予创建应用程序的权限	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
CreateApplicationPresignedUrl	授予权限以创建和返回可用于连接应用程序扩展的 URL	Read	application*		
CreateApplicationSnapshot	授予权限以为应用程序创建快照	Write	application*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteApplication	授予权限以删除应用程序	Write	application*		
DeleteApplicationCloudWatchLoggingOption	授予权限以删除应用程序的指定 cloudwatch 日志记录选项	Write	application*		
DeleteApplicationInputProcessingConfiguration	授予权限以删除应用程序的指定输入处理配置	Write	application*		
DeleteApplicationOutput	授予权限以删除应用程序的指定输出	Write	application*		
DeleteApplicationReferenceDataSource	授予权限以删除应用程序的指定引用数据源	Write	application*		
DeleteApplicationSnapshot	授予权限以删除应用程序快照	Write	application*		
DeleteApplicationVpcConfiguration	授予权限以删除应用程序的指定 VPC 配置	Write	application*		
DescribeApplication	授予权限以描述指定应用程序	读取	application*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeApplicationOperation	授予权限以描述应用程序的应用程序操作	读取	application*		
DescribeApplicationSnapshot	授予权限以描述应用程序快照	读取	application*		
DescribeApplicationVersion	授予权限以描述应用程序的版本	读取	application*		
DiscoverInputSchema	授予权限以发现应用程序输入架构	读取			iam:PassRole
ListApplicationOperations	授予权限以列出应用程序的应用程序操作	读取	application*		
ListApplicationSnapshots	授予权限以列出应用程序快照	读取	application*		
ListApplicationVersions	授予权限以列出应用程序的版本	读取	application*		
ListApplications	授予权限以列出账户应用程序	List			
ListTagsForResource	授予权限以获取与应用程序关联的标签	读取	application*		
RollbackApplication	授予对应用程序执行回滚操作的权限	写入	application*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StartApplication	授予权限以启动应用程序	Write	application*		
StopApplication	授予权限以停止应用程序	Write	application*		
TagResource	授予权限以向应用程序添加标签	Tagging	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予权限以从应用程序中删除指定标签	Tagging	application*		
				aws:TagKeys	
UpdateApplication	授予权限以更新应用程序	写入	application*		
UpdateApplicationMaintenanceConfiguration	授予权限以更新应用程序的维护配置	写入	application*		

Amazon Kinesis Analytics V2 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从

而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
application	`arn:${Partition}:kinesisanalytics:${Region}:${Account}:application/${ApplicationName}`	aws:ResourceTag/${TagKey}

Amazon Kinesis Analytics V2 的条件键

Amazon Kinesis Analytics V2 定义以下可以在 IAM policy 的 `Condition` 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按每个标签的值集筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签值筛选访问权限	字符串
aws:TagKeys	按请求中是否有必需标签键来筛选访问权限	ArrayOfString

Amazon Kinesis Data Streams 的操作、资源和条件键

Amazon Kinesis Data Streams（服务前缀：`kinesis`）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon Kinesis Data Streams 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddTagsToStream	授予为指定 Amazon Kinesis 流添加或更新标签的权限 每个流可最多可以有 10 个标签	标记	stream*	aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
CreateStream	授予创建 Amazon Kinesis 流的权限	写入	stream*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
DecreaseStreamRetentionPeriod	授予缩短流的保留期的权限，保留期是将数据记录添加到流中后可供访问的期限。	写入	stream*	aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	授予删除与指定流或使用者关联的资源策略的权限	写入	consumer*		
			stream*	aws:ResourceTag/${TagKey}	
DeleteStream	授予删除流及其所有分片和数据的权限	写入	stream*	aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeregisterStreamConsumer	授予从 Kinesis 数据流取消注册流使用者的权限。	写入	consumer*		
DescribeLimits	授予描述账户的分片限制和使用量的权限	读取			
DescribeStream	授予描述指定流的权限	读取	stream*	aws:ResourceTag/${TagKey}	
DescribeStreamConsumer	授予获取注册的流使用者描述的权限	读取	consumer*		
DescribeStreamSummary	授予提供无分片列表的指定 Kinesis 数据流的摘要描述的权限	读取	stream*	aws:ResourceTag/${TagKey}	
DisableEnhancedMonitoring	授予禁用增强监控的权限	写入			
EnableEnhancedMonitoring	授予对分片级别指标启用增强型 Kinesis 数据流监控的权限	写入			
GetRecords	授予获取分片中数据记录的权限	读取	stream*	aws:ResourceTag/${TagKey}	
GetResourcePolicy	授予获取与指定流或使用者关联的资源策略的权限	读取	consumer*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			stream*	aws:ResourceTag/${TagKey}	
GetShardIterator	授予获取分片迭代器的权限。分片迭代器将在其返回给请求者的五分钟后过期。	读取	stream*	aws:ResourceTag/${TagKey}	
IncreaseStreamRetentionPeriod	授予增加流的保留期的权限，保留期是将数据记录添加到流中后可供访问的期限。	写入	stream*	aws:ResourceTag/${TagKey}	
ListShards	授予列出流中的分片，并提供有关每个分片的信息的权限。	列表	stream*	aws:ResourceTag/${TagKey}	
ListStreamConsumers	授予列出使用增强型扇出从 Kinesis 流中接收数据的注册流使用者，并提供有关每个使用者的信息的权限。	列表	stream*	aws:ResourceTag/${TagKey}	
ListStreams	授予列出流的权限	列表			
ListTagsForStream	授予列出指定 Amazon Kinesis 流的标签的权限	读取	stream*	aws:ResourceTag/${TagKey}	
MergeShards	授予将两个相邻分片合并为一个流并将其组合为单一分片，从而减少流接收和传输数据的容量的权限。	写入	stream*	aws:ResourceTag/${TagKey}	
PutRecord	授予将来自创建器的单个数据记录写入 Amazon Kinesis 流中的权限	写入	stream*	aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutRecords	授予通过一次调用（也称为请求）将来自生产者的多条数据记录写入 Amazon Kinesis 流的 PutRecords 权限	写入	stream*	aws:ResourceTag/${TagKey}	
PutResourcePolicy	授予将资源策略附加到指定流或使用者的权限	写入	consumer*		
			stream*	aws:ResourceTag/${TagKey}	
RegisterStreamConsumer	授予将流使用者注册到 Kinesis 数据流的权限。	写入	stream*	aws:ResourceTag/${TagKey}	
RemoveTagsFromStream	授予从指定 Kinesis 数据流移除标签的权限。移除的标签将被删除且在此操作成功完成后将无法恢复	标记	stream*	aws:TagKeys aws:ResourceTag/${TagKey}	
SplitShard	授予将一个分片分割为 Kinesis 数据流中的两个新分片，从而增加流接收和传输数据的容量的权限	写入	stream*	aws:ResourceTag/${TagKey}	
StartStreamEncryption	授予使用 KMS 密 Amazon 钥为指定流启用或更新服务器端加密的权限	写入	kmsKey*		
			stream*	aws:ResourceTag/${TagKey}	
StopStreamEncryption	授予为指定流禁用服务器端加密的权限	写入	kmsKey*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			stream*	aws:ResourceTag/${TagKey}	
SubscribeToShard	授予侦听具有增强型扇出的特定分片的权限	读取	consumer*		
UpdateShardCount	授予将指定流的分片数更新为指定分片数的权限	写入			
UpdateStreamMode	授予更新数据流的容量模式的权限	写入			

Amazon Kinesis Data Streams 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
stream	arn:${Partition}:kinesis:${Region}:${Account}:stream/${StreamName}	aws:ResourceTag/${TagKey}
consumer	arn:${Partition}:kinesis:${Region}:${Account}:${StreamType}/${StreamName}/consumer/${ConsumerName}:${ConsumerCreationTimpstamp}	
kmsKey	arn:${Partition}:kms:${Region}:${Account}:key/${KeyId}	

Amazon Kinesis Data Streams 的条件键

Amazon Kinesis Data Streams 定义以下可以在 IAM 策略的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对来筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按附加到资源的标签键值对筛选操作	字符串
aws:TagKeys	根据在请求中是否具有标签键来筛选访问	ArrayOfString

Amazon Kinesis Firehose 的操作、资源和条件键

Amazon Kinesis Firehose（服务前缀：firehose）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Kinesis Firehose 定义的操作
- Amazon Kinesis Firehose 定义的资源类型
- Amazon Kinesis Firehose 的条件键

Amazon Kinesis Firehose 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateDeliveryStream	授予权限以创建传输流	写入	deliverystream*		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteDeliveryStream	授予权限以删除传输流及其数据	Write	deliverystream*		
DescribeDeliveryStream	授予权限以描述指定传输流并获取状态	读取	deliverystream*		
ListDeliveryStreams	授予权限以列出传输流	列表			
ListTagsForDeliveryStream	授予权限以列出指定传输流标签	列表	deliverystream*		
PutRecord	授予权限以将单个数据记录写入 Amazon Kinesis Firehose 传输流	写入	deliverystream*		
PutRecordBatch	授予权限以在一次调用中将多条数据记录写入传输流，这样可以实现比写入单条记录更高的每个创建者吞吐量	写入	deliverystream*		
StartDeliveryStreamEncryption	授予权限以为传输流启用服务器端加密（SSE）	写入	deliverystream*		
StopDeliveryStreamEncryption	授予权限以禁用指定传输流的指定目标	写入	deliverystream*		
TagDeliveryStream	授予权限以为指定传输流添加或更新标签	标记	deliverystream*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagDeliveryStream	授予权限以从指定传输流中删除标签	标记	deliverystream*		
				aws:TagKeys	
UpdateDestination	授予权限以更新指定传输流的指定目标	写入	deliverystream*		

Amazon Kinesis Firehose 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
deliverystream	arn:${Partition}:firehose:${Region}:${Account}:deliverystream/${DeliveryStreamName}	aws:ResourceTag/${TagKey}

Amazon Kinesis Firehose 的条件键

Amazon Kinesis Firehose 定义以下可以在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString

Amazon Kinesis Video Streams 的操作、资源和条件键

Amazon Kinesis Video Streams（服务前缀：`kinesisvideo`）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Kinesis Video Streams 定义的操作
- Amazon Kinesis Video Streams 定义的资源类型
- Amazon Kinesis Video Streams 的条件键

Amazon Kinesis Video Streams 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，

以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ConnectAsMaster	授予权限，从而以主用户的身份连接到终端节点指定的信令通道	Write	channel*		
ConnectAsViewer	授予权限，从而以查看者的身份连接到终端节点指定的信令通道	Write	channel*		
CreateSignalingChannel	授予权限以创建信令通道	Write	channel*		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateStream	授予权限以创建 Kinesis 视频流	写入	stream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteEdgeConfiguration	授予删除 Kinesis 视频流边缘配置的权限	写入	stream*		
DeleteSignalingChannel	授予权限以删除现有信令通道	Write	channel*		
DeleteStream	授予权限以删除现有 Kinesis 视频流	写入	stream*		
DescribeEdgeConfiguration	授予权限以描述您 Kinesis 视频流的边缘配置	读取	stream*		
DescribeImageGenerationConfiguration	授予权限以描述您 Kinesis 视频流的映像生成配置	读取	stream*		
DescribeMappedResourceConfiguration	授予描述映射到 Kinesis 视频流的资源的权限	列表	stream*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeMediaStorageConfiguration	授予描述信令通道的媒体存储配置的权限	读取	channel*		
DescribeNotificationConfiguration	授予权限以描述您 Kinesis 视频流的通知配置	读取	stream*		
DescribeSignalingChannel	授予权限以描述指定的信令通道	List	channel*		
DescribeStream	授予权限以描述指定的 Kinesis 视频流	List	stream*		
GetClip	授予权限以从视频流中获取媒体剪辑	Read	stream*		
GetDASHStreamingSessionURL	授予权限以便为 MPEG-DASH 视频流创建 URL	Read	stream*		
GetDataEndpoint	授予权限以获取指定流的终端节点，用于对 Kinesis Video Streams 读取或写入媒体数据。	Read	stream*		
GetHLSStreamingSessionURL	授予权限以便为 HLS 视频流创建 URL	Read	stream*		
GetIceServerConfig	授予权限以获取 ICE 服务器配置	读取	channel*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetImages	授予权限以从您 Kinesis 视频流中获取生成的映像	读取	stream*		
GetMedia	授予权限以返回 Kinesis 视频流的媒体内容	Read	stream*		
GetMediaForFragmentList	授予权限以仅读取并返回持久性存储中的媒体数据。	Read	stream*		
GetSignalingChannelEndpoint	授予权限以获取信令通道的具有指定协议和角色组合的终端节点	读取	channel*		
JoinStorageSession	授予加入通道的存储会话的权限	写入	channel*		
JoinStorageSessionAsViewer	授予权限以作为查看器加入通道的存储会话	写入	channel*		
ListEdgeAgentConfigurations	授予列出边缘代理配置的权限	列表			
ListFragments	授予权限以根据指定了范围的分页标记或选择器类型，列出存档存储中的片段。	List	stream*		
ListSignalingChannels	授予权限以列出您的信令通道	List			
ListStreams	授予权限以列出您的 Kinesis 视频流	List			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListTagsForResource	授予权限以提取与您的资源关联的标签	Read	channel		
			stream		
ListTagsForStream	授予权限以提取与 Kinesis 视频流关联的标签	Read	stream*		
PutMedia	授予权限以将媒体数据发送到 Kinesis 视频流	Write	stream*		
SendAlexaOfferToMaster	授予权限以将 Alexa SDP 方案发送给主用户	写入	channel*		
StartEdgeConfigurationUpdate	授予权限以开始您 Kinesis 视频流的边缘配置更新	写入	stream*		
TagResource	授予权限以将一组标签附加到资源	Tagging	channel		
			stream		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagStream	授予权限以将一组标签附加到 Kinesis 视频流	Tagging	stream*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予权限以从您的资源删除一个或多个标签	Tagging	channel		
			stream		
				aws:TagKeys	
UntagStream	授予权限以从 Kinesis 视频流中删除一个或多个标签	Tagging	stream*		
				aws:TagKeys	
UpdateDataRetention	授予权限以更新 Kinesis 视频流的数据保留期限	写入	stream*		
UpdateImageGenerationConfiguration	授予权限以更新您 Kinesis 视频流的映像生成配置	写入	stream*		
UpdateMediaStorageConfiguration	授予创建或更新信令通道和流之间映射的权限	写入	channel*		
UpdateNotificationConfiguration	授予权限以更新您 Kinesis 视频流的通知配置	写入	stream*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateSignalingChannel	授予权限以更新现有信令通道	Write	channel*		
UpdateStream	授予权限以更新现有 Kinesis 视频流	Write	stream*		

Amazon Kinesis Video Streams 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
stream	arn:${Partition}:kinesisvideo:${Region}:${Account}:stream/${StreamName}/${CreationTime}	aws:ResourceTag/${TagKey}
channel	arn:${Partition}:kinesisvideo:${Region}:${Account}:channel/${ChannelName}/${CreationTime}	aws:ResourceTag/${TagKey}

Amazon Kinesis Video Streams 的条件键

Amazon Kinesis Video Streams 定义以下可以在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据每个标签的允许值集筛选请求	字符串
aws:ResourceTag/${TagKey}	根据与流关联的标签值筛选操作	字符串
aws:TagKeys	根据在请求中是否具有必需标签键以筛选请求	ArrayOfString

Amazon Lambda 的操作、资源和条件键

Amazon Lambda（服务前缀:lambda）提供以下特定于服务的资源、操作和条件上下文密钥以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Lambda 定义的操作
- Amazon Lambda 定义的资源类型
- Amazon Lambda 的条件键

Amazon Lambda 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须

具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddLayerVersionPermission	授予向某个 Lamb Amazon da 层版本的基于资源的策略添加权限的权限	权限管理	layerVersion*		
AddPermission	授予权限以授予 Amazon 服务或其他账户使用 Amazon Lambda 函数的权限	权限管理	function*		
				lambda:Principal lambda:FunctionUrlAuthType	
CreateAlias	授予权限以创建 Lambda 函数版本的别名	写入	function*		
CreateCodeSigningConfig	授予创建 Amazon Lambda 代码签名配置的权限	写入		aws:RequestTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys	
CreateEventSourceMapping	授予在事件源和 Amazon Lambda 函数之间创建映射的权限	写入		lambda:FunctionArn aws:RequestTag/${TagKey} aws:TagKeys	
CreateFunction	授予创建 Amazon Lambda 函数的权限	写入	function*		iam:PassRole

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				lambda:Layer lambda:VpcIds lambda:SubnetIds lambda:SecurityGroupIds lambda:CodeSigningConfigArn aws:RequestTag/${TagKey} aws:TagKeys	
CreateFunctionUrlConfig	授予权限以创建 Lambda 函数的函数 url 配置	写入	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	
DeleteAlias	授予删除 Amazon Lambda 函数别名的权限	写入	function*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteCodeSigningConfig	授予删除 Amazon Lambda 代码签名配置的权限	写入	code signing config*		
DeleteEventSourceMapping	授予删除 Amazon Lambda 事件源映射的权限	写入	eventSourceMapping*		
				lambda:FunctionArn	
DeleteFunction	授予删除 Amazon Lambda 函数的权限	写入	function*		
DeleteFunctionCodeSigningConfig	授予将代码签名配置与 Lamb Amazon da 函数分离的权限	写入	function*		
DeleteFunctionConcurrency	授予从 Amazon Lambda 函数中移除并发执行限制的权限	写入	function*		
DeleteFunctionEventInvokeConfig	授予删除 Lambd Amazon a 函数、版本或别名的异步调用配置的权限	写入	function*		
DeleteFunctionUrlConfig	授予权限以删除 Lambda 函数的函数 url 配置	写入	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteLayerVersion	授予删除 Amazon Lambda 层版本的权限	写入	layerVersion*		
DeleteProvisionedConcurrencyConfig	授予删除 Lambda 函数 Amazon 的预配置并发配置的权限	写入	function alias		
			function version		
DisableReplication[仅权限]	授予权限以禁用 Lambda@Edge 函数复制	Permissions management	function*		
EnableReplication[仅权限]	授予权限以启用 Lambda@Edge 函数复制	权限管理	function*		
GetAccountSettings	授予在账户中查看有关账户限制和使用情况的详细信息的权限 Amazon Web Services 区域	读取			
GetAlias	授予查看有关 Amazon Lambda 函数别名的详细信息的权限	读取	function*		
GetCodeSigningConfig	授予查看有关 Amazon Lambda 代码签名配置详细信息的权限	读取	code signing config*		
GetEventSourceMapping	授予权限以查看有关 Amazon Lambda 事件源映射的详细信息	读取	eventSourceMapping*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				lambda:FunctionArn	
GetFunction	授予查看有关 Amazon Lambda 函数详细信息的权限	读取	function*		
GetFunctionCodeSigningConfig	授予查看附加到 Lamb Amazon da 函数的代码签名配置 arn 的权限	读取	function*		
GetFunctionConcurrency	授予权限以查看有关函数的保留并发配置的详细信息	读取	function*		
GetFunctionConfiguration	授予权限以查看有关 Lambda 函数 Amazon 或版本的特定版本设置的详细信息	读取	function*		
GetFunctionEventInvokeConfig	授予权限以查看函数、版本或别名的异步调用配置	读取	function*		
GetFunctionRecursionConfig	授予查看 Lamb Amazon da 函数递归配置的权限	读取	function*		
GetFunctionUrlConfig	授予权限以读取 Lambda 函数的函数 url 配置	读取	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetLayerVersion	授予查看有关 Amazon Lambda 层版本详细信息的权限。请注意，此操作还支持 GetLayerVersionByArn API	读取	layerVersion*		
GetLayerVersionPolicy	授予查看 Lamb Amazon da 层版本的基于资源的策略的权限	读取	layerVersion*		
GetPolicy	授予查看 Lambd Amazon a 函数、版本或别名的基于资源的策略的权限	读取	function*		
GetProvisionedConcurrencyConfig	授予查看 Lambd Amazon a 函数别名或版本的预配置并发配置的权限	读取	functionalias		
			functionversion		
GetRuntimeManagementConfig	授予查看 Amazon Lambda 函数运行时管理配置的权限	读取	function*		
InvokeAsync	授予权限以异步调用函数（已弃用）	写入	function*		
InvokeFunction	授予调用 Amazon Lambda 函数的权限	写入	function*		
				lambda:EventSourceToken	
InvokeFunctionUrl[仅权限]	授予通过网址调用 L Amazon ambda 函数的权限	写入	function*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				lambda:FunctionUrlAuthType lambda:FunctionArn lambda:EventSourceToken	
ListAliases	授予检索 Lamb Amazon da 函数别名列表的权限	列表	function*		
ListCodeSigningConfigs	授予检索 Amazon Lambda 代码签名配置列表的权限	列表			
ListEventSourceMappings	授予检索 Amazon Lambda 事件源映射列表的权限	列表			
ListFunctionEventInvokeConfigs	授予权限以检索函数异步调用的配置列表	列表	function*		
ListFunctionUrlConfigs	授予权限以读取函数的函数 url 配置	列表	function*		
				lambda:FunctionUrlAuthType	
ListFunctions	授予检索 Amazon Lambda 函数列表的权限，以及每个函数的版本特定配置	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListFunctionsByCodeSigningConfig	授予通过分配的代码签名配置检索 Amazon Lambda 函数列表的权限	列表	code signing config*		
ListLayerVersions	授予检索 Amazon Lambda 层版本列表的权限	列表			
ListLayers	授予检索 Amazon Lambda 层列表的权限，以及有关每个层最新版本的详细信息	列表			
ListProvisionedConcurrencyConfigs	授予检索 Lambda 函数 Amazon 的预配置并发配置列表的权限	列表	function*		
ListTags	授予检索 Amazon Lambda 函数、事件源映射或代码签名配置资源的标签列表的权限	读取	code signing config		
			eventSourceMapping		
			function		
ListVersionsByFunction	授予检索 Amazon Lambda 函数版本列表的权限	列表	function*		
PublishLayerVersion	授予创建 Amazon Lambda 层的权限	写入	layer*		
PublishVersion	授予创建 Amazon Lambda 函数版本的权限	写入	function*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutFunctionCodeSigningConfig	授予将代码签名配置附加到 Amazon Lambda 函数的权限	写入	code signing config*		
			function*		
				lambda:CodeSigningConfigArn	
PutFunctionConcurrency	授予为 Lamb Amazon da 函数配置预留并发的权限	写入	function*		
PutFunctionEventInvokeConfig	授予对 Lambd Amazon a 函数、版本或别名配置异步调用选项的权限	写入	function*		
PutFunctionRecursionConfig	授予更新 Lamb Amazon da 函数递归配置的权限	写入	function*		
PutProvisionedConcurrencyConfig	授予为 Lambd Amazon a 函数的别名或版本配置预配置并发的权限	写入	function alias		
			function version		
PutRuntimeManagementConfig	授予更新 Amazon Lambda 函数运行时管理配置的权限	写入	function*		
RemoveLayerVersionPermission	授予从 Amazon Lambda 层版本的权限策略中删除语句的权限	权限管理	layerVersion*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
RemovePermission	授予撤销 Amazon 服务或其他账号的功能使用权限的权限	权限管理	function*		
				lambda:PrincipalOrgID lambda:FunctionUrlAuthType	
TagResource	授予向 Amazon Lambda 函数、事件源映射或代码签名配置资源添加标签的权限	标记	codesigningconfig		
			eventSourceMapping		
			function		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予从 Amazon Lambda 函数、事件源映射或代码签名配置资源中移除标签的权限	标记	codesigningconfig		
			eventSourceMapping		
			function		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys	
UpdateAlias	授予更新 Amazon Lambda 函数别名配置的权限	写入	function*		
UpdateCodeSigningConfig	授予更新 Amazon Lambda 代码签名配置的权限	写入	codesigningconfig*		
UpdateEventSourceMapping	授予更新 Amazon Lambda 事件源映射配置的权限	写入	eventSourceMapping*		
				lambda:FunctionArn	
UpdateFunctionCode	授予更新 Amazon Lambda 函数代码的权限	写入	function*		
UpdateFunctionCodeSigningConfig	授予更新 Amazon Lambda 函数代码签名配置的权限	写入	codesigningconfig*		
			function*		
UpdateFunctionConfiguration	授予修改 Lambda 函数 Amazon 特定版本设置的权限	写入	function*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				lambda:Layer lambda:VpcIds lambda:SubnetIds lambda:SecurityGroupIds	
UpdateFunctionEventInvokeConfig	授予修改异步调用 Lambd Amazon a 函数、版本或别名的配置的权限	写入	function*		
UpdateFunctionUrlConfig	授予权限以更新 Lambda 函数的函数 url 配置	写入	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	

Amazon Lambda 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
code signing config	arn:${Partition}:lambda:${Region}:${Account}:code-signing-config:${CodeSigningConfigId}	aws:ResourceTag/${TagKey}
eventSourceMapping	arn:${Partition}:lambda:${Region}:${Account}:event-source-mapping:${UUID}	aws:ResourceTag/${TagKey}
function	arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}	aws:ResourceTag/${TagKey}
function alias	arn:${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}	

Amazon Lambda 的条件键

Amazon Lambda 定义了以下可在 IAM 策略Condition元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString
lambda:CodeSigningConfigArn	通过 Lambda Amazon 代码签名配置的 ARN 筛选访问权限	ARN
lambda:EventSourceToken	按照 ID 筛选来自为 Amazon Lambda 函数配置的非Amazon 事件源的访问权限	字符串
lambda:FunctionArn	通过 Lambda 函数 Amazon 的 ARN 筛选访问权限	ARN
lambda:FunctionUrlAuthType	按请求中指定的授权类型筛选访问。在 CreateFunctionUrlConfig、、 UpdateFunctionUrlConfig、 DeleteFunctionUrlConfig GetFunctionUrlConfig ListFunctionUrlConfig、 AddPermission 和 RemovePermission 操作期间可用	字符串
lambda:Layer	按 Lambda Amazon 层版本的 ARN 筛选访问权限	ArrayOfString
lambda:Principal	通过限制可以调用函数的 Amazon 服务或账号来筛选访问权限	字符串
lambda:SecurityGroupIds	根据为 Amazon Lambda 函数配置的安全组的 ID 筛选访问权限	ArrayOfString
lambda:SourceFunctionArn	按发起请求的 Lambd Amazon a 函数的 ARN 筛选访问权限	ARN
lambda:SubnetIds	根据为 Lamb Amazon da 函数配置的子网 ID 筛选访问权限	ArrayOfString

条件键	描述	类型
lambda:VpcIds	根据为 Amazon Lambda 函数配置的 VPC 的 ID 筛选访问权限	字符串

Amazon Launch Wizard 的操作、资源和条件键

Amazon Launch Wizard（服务前缀:`launchwizard`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Launch Wizard 定义的操作
- Amazon Launch Wizard 定义的资源类型
- Amazon Launch Wizard 的条件键

Amazon Launch Wizard 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateAdditionalNode[仅权限]	授予创建其他节点的权限	写入			
CreateDeployment	授予创建部署的权限	写入	deployment*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateSettingsSet[仅权限]	授予创建应用程序设置集的权限	写入			
DeleteAdditionalNode[仅权限]	授予删除其他节点的权限	写入			
DeleteApp[仅权限]	授予删除应用程序的权限	写入			
DeleteDeployment	授予删除部署的权限	写入	deployment*	aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteSettingsSet[仅权限]	授予删除设置集的权限	写入			
DescribeAdditionalNode[仅权限]	授予描述其他节点的权限	读取			
DescribeProvisionedApp[仅权限]	授予描述预置应用程序的权限	读取			
DescribeProvisioningEvents[仅权限]	授予描述预置事件的权限	读取			
DescribeSettingsSet[仅权限]	授予描述应用程序设置集的权限	读取			
GetDeployment	授予获取部署的权限	读取	deployment*	aws:ResourceTag/${TagKey}	
GetInfrastructureSuggestion[仅权限]	授予获取基础设施建议的权限	读取			
GetIpAddress[仅权限]	授予获取客户 IP 地址的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetResourceCostEstimate[仅权限]	授予获取资源成本估算的权限	读取			
GetResourceRecommendation[仅权限]	授予获取资源的建议的权限	读取			
GetSettingsSet[仅权限]	授予获取设置集的权限	读取			
GetWorkload	授予获取工作负载的权限	读取			
GetWorkloadAsset[仅权限]	授予获取工作负载的资产的权限	读取			
GetWorkloadAssets[仅权限]	授予获取工作负载资产的权限	读取			
GetWorkloadDeploymentPattern	授予权限以获取部署模式	读取			
ListAdditionalNodes[仅权限]	授予列出其他节点的权限	列表			
ListAllowedResources[仅权限]	授予列出允许的资源的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListDeploymentEvents	授予列出部署期间发生的事件的权限	列表			
ListDeployments	授予列出部署的权限	列表			
ListProvisionedApps[仅权限]	授予列出预置应用程序的权限	列表			
ListResourceCostEstimates[仅权限]	授予列出资源成本估算的权限	列表			
ListSettingsSets[仅权限]	授予列出设置集的权限	列表			
ListTagsForResource	授予列出 LaunchWizard 资源标签的权限。	读取	deployment	aws:ResourceTag/${TagKey}	
ListWorkloadDeploymentOptions[仅权限]	授予列出给定工作负载的部署选项的权限	列表			
ListWorkloadDeploymentPatterns	授予列出工作负载的部署模式的权限	列表			
ListWorkloads	授予列出工作负载的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutSettingsSet[仅权限]	授予创建设置集的权限	写入			
StartProvisioning[仅权限]	授予启动预置的权限。	写入			
TagResource	授予为 LaunchWizard 资源添加标签的权限。	标记	deployment	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	授予取消标记 LaunchWizard 资源的权限。	标记	deployment	aws:TagKeys	
UpdateSettingsSet[仅权限]	授予更新应用程序设置集的权限	写入			

Amazon Launch Wizard 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
deployment	arn:${Partition}:launchwizard:${Region}:${Account}:deployment/${DeploymentId}	aws:ResourceTag/${TagKey}

Amazon Launch Wizard 的条件键

Amazon Launch Wizard 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对来筛选访问权限	字符串
aws:ResourceTag/${TagKey}	根据附加到资源的标签键值对筛选访问	字符串
aws:TagKeys	根据在请求中是否具有标签键来筛选访问权限	ArrayOfString

Amazon License Manager 的操作、资源和条件键

Amazon License Manager（服务前缀:license-manager）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon License Manager 定义的操作
- Amazon License Manager 定义的资源类型
- Amazon License Manager 的条件键

Amazon License Manager 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AcceptGrant	授予接受授予的权限	Write	grant*		
CheckInLicense	授予将许可证授权签入回池的权限	Write			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CheckoutBorrowLicense	授予签出许可证授权以用于借用使用案例的权限	Write	license*		
CheckoutLicense	授予签出许可证授权的权限	Write			
CreateGrant	授予创建新许可证授权的权限	Write	license*		
CreateGrantVersion	授予创建新版本授权的权限	Write	grant*		
CreateLicense	授予创建新许可证的权限	Write			
CreateLicenseConfiguration	授予权限以创建新许可证配置	写入		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicenseConversionTaskForResource	授予为资源创建许可证转换任务的权限	写入			
CreateLicenseManagerReportGenerator	授予权限以为许可证配置创建报告生成器	写入		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicenseVersion	授予创建许可证新版本的权限	写入	license*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateToken	授予为许可证创建新令牌的权限	写入	license*		
DeleteGrant	授予权限以删除授权	写入	grant*		
DeleteLicense	授予删除许可证的权限	Write	license*		
DeleteLicenseConfiguration	授予永久删除许可证配置的权限	Write	license-configuration*		
DeleteLicenseManagerReportGenerator	授予删除报告生成器的权限	Write	report-generator*		
DeleteToken	授予删除令牌的权限	Write			
ExtendLicenseConsumption	授予延长已签出许可证授权的使用期限的权限	Write			
GetAccessToken	授予获取访问令牌的权限	Read			
GetGrant	授予获取授权的权限	Read	grant*		
GetLicense	授予获取许可证的权限	Read	license*		
GetLicenseConfiguration	授予获取许可证配置的权限	读取	license-configuration*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetLicenseConversionTask	授予权限以检索许可证转换任务	读取			
GetLicenseManagerReportGenerator	授予获取报告生成器的权限	Read	report-generator*		
GetLicenseUsage	授予获取许可证使用情况的权限	Read	license*		
GetServiceSettings	授予获取服务设置的权限	List			
ListAssociationsForLicenseConfiguration	授予列出所选许可证配置的关联的权限	List	license-configuration*		
ListDistributedGrants	授予列出分布式授权的权限	List			
ListFailuresForLicenseConfigurationOperations	授予列出失败的许可证配置操作的权限	List	license-configuration*		
ListLicenseConfigurations	授予权限以列出许可证配置	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListLicenseConversionTasks	授予列出许可证转换任务的权限	列表			
ListLicenseManagerReportGenerators	授予列出报告生成器的权限	List	license-configuration		
ListLicenseSpecificationsForResource	授予列出与所选资源关联的许可证规范的权限	List			
ListLicenseVersions	授予列出许可证版本的权限	List	license*		
ListLicenses	授予权限以列出许可证	读取			
ListReceivedGrants	授予权限以列出所收到的授权	列表			
ListReceivedGrantsForOrganization	授予权限以列出组织所收到的授权	列表			
ListReceivedLicenses	授予列出所收到的许可证的权限	列表			
ListReceivedLicensesForOrganization	授予权限以列出组织所收到的许可证	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListResourceInventory	授予列出资源清单的权限	List			
ListTagsForResource	授予权限以列出所选资源标签	读取	license-configuration*		
ListTokens	授予权限以列出令牌	List			
ListUsageForLicenseConfiguration	授予列出所选许可证配置的使用情况记录的权限	List	license-configuration*		
RejectGrant	授予拒绝授权的权限	Write	grant*		
TagResource	授予标记所选资源的权限	Tagging	license-configuration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予取消标记所选资源的权限	Tagging	license-configuration*		
UpdateLicenseConfiguration	授予更新现有许可证配置的权限	Write	license-configuration*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateLicenseManagerReportGenerator	授予更新许可证配置的报告生成器的权限	Write	report-generator*		
UpdateLicenseSpecificationsForResource	授予更新所选资源的许可证规范的权限	Write	license-configuration*		
UpdateServiceSettings	授予更新服务设置的权限	Permissions management			

Amazon License Manager 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
license-configuration	arn:${Partition}:license-manager:${Region}:${Account}:license-configuration:${LicenseConfigurationId}	license-manager:ResourceTag/${TagKey}
license	arn:${Partition}:license-manager::${Account}:license:${LicenseId}	
grant	arn:${Partition}:license-manager::${Account}:grant:${GrantId}	

资源类型	ARN	条件键
report-generator	arn:${Partition}:license-manager:${Region}:${Account}:report-generator:${ReportGeneratorId}	license-manager:ResourceTag/${TagKey}

Amazon License Manager 的条件键

Amazon License Manager 定义了以下条件密钥，这些条件密钥可用于 IAM 策略的Condition元素中。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString
license-manager:ResourceTag/${TagKey}	按附加到资源的标签键值对筛选访问权限	字符串

Amazon License Manager Linux Subscriptions Manager 的操作、资源和条件键

Amazon License Manager Linux 订阅管理器（服务前缀:license-manager-linux-subscriptions）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。

- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon License Manager Linux Subscriptions Manager 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeregisterSubscriptionProvider	授予在 License Manager 中永久删除订阅提供商的 Amazon 权限	写入	subscription-provider*		
GetRegisteredSubscriptionProvider	授予在 License Manager 中获取订阅提供商的 Amazon 权限	读取	subscription-provider*		
GetServiceSettings	授予在 Amazon 许可证管理器中获取 Linux 订阅服务设置的权限	读取			
ListLinuxSubscriptionInstances	授予在 License Manager 中 Amazon 列出所有订阅 Linux 的实例的权限	读取			
ListLinuxSubscriptions	授予在 License Manager 中列出所有 Linux 订阅的 Amazon 权限	读取			
ListRegisteredSubscriptionProviders	授予在 License Manager 中列出订阅提供商的 Amazon 权限	读取			
ListTagsForResource	授予权限以列出所选资源标签	读取	subscription-provider*		
RegisterSubscriptionProvider	授予在 License Manager 中创建新订阅提供商的 Amazon 权限	写入		aws:RequestTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys	
TagResource	授予标记所选资源的权限	Tagging	subscription-provider*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予取消标记所选资源的权限	标记	subscription-provider*		
				aws:TagKeys	
UpdateServiceSettings	授予在 License Manager 中 Amazon 更新 Linux 订阅服务设置的权限	写入			

Amazon License Manager Linux Subscriptions Manager 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
subscription-provider	arn:${Partition}:license-manager-linux-subscriptions:${Region}:${Account}:subscription-provider/${SubscriptionProviderId}	aws:ResourceTag/${TagKey}

Amazon License Manager Linux Subscriptions Manager 的条件键

Amazon License Manager Linux 订阅管理器定义了以下条件密钥，这些条件密钥可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按附加到资源的标签键值对筛选操作	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString

Amazon Managed Streaming for Apache Kafka 的操作、资源和条件键

Amazon Managed Streaming for Apache Kafka（服务前缀：kafka）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon Managed Streaming for Apache Kafka 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchAssociateScramSecret	授予将一个或多个 Scram 密钥与 Amazon MSK 集群关联的权限	Write	cluster*		kms:CreateGrant

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
					kms:RetireGrant
BatchDisassociateScramSecret	授予取消一个或多个 Scram 密钥与 Amazon MSK 集群的关联的权限	Write	cluster*		kms:RetireGrant
CreateCluster	授予创建 MSK 集群的权限	写入	cluster*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy kms:CreateGrant kms:DescribeKey

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateClusterV2	授予创建 MSK 集群的权限	Write	cluster*		ec2:CreateTags ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs iam:AttachRolePolicy

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
					iam:CreateServiceLinkedRole iam:PutRolePolicy kms:CreateGrant kms:DescribeKey
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfiguration	授予创建 MSK 配置的权限	写入	configuration*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateReplicator	授予权限以创建 MSK 复制程序	写入	replicator*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PassRole iam:PutRolePolicy kafka:DescribeClusterV2 kafka:GetBootstrapBrokers

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateVpcConnection	授予创建 MSK VPC 连接的权限	写入	cluster*		ec2:CreateTags ec2:CreateVpcEndpoint ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs iam:AttachRolePolicy iam:CreateServiceLinkedRole

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
					iam:PutRolePolicy
			vpc-connection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCluster	授予删除 MSK 集群的权限	写入	cluster*		ec2:DeleteVpcEndpoints ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints
DeleteClusterPolicy	授予权限以删除集群基于资源的策略	写入	cluster*		
DeleteConfiguration	授予删除指定 MSK 配置的权限	写入	configuration*		
DeleteReplicator	授予权限以删除 MSK 复制程序	写入	replicator*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteVpcConnection	授予删除 MSK VPC 连接的权限	写入	vpc-connection*		ec2:DeleteVpcEndpoints ec2:DescribeVpcEndpoints
DescribeCluster	授予描述 MSK 集群的权限	Read	cluster*		
DescribeClusterOperation	授予描述给定 ARN 指定的集群操作的权限	读取			
DescribeClusterOperationV2	授予描述给定 ARN 指定的集群操作的权限	读取			
DescribeClusterV2	授予描述 MSK 集群的权限	读取	cluster*		
DescribeConfiguration	授予描述 MSK 配置的权限	Read	configuration*		
DescribeConfigurationRevision	授予描述 MSK 配置修订的权限	读取	configuration*		
DescribeReplicator	授予权限以描述 MSK 复制程序	读取	replicator*		
DescribeVpcConnection	授予描述 MSK VPC 连接的权限	读取	vpc-connection*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetBootstrapBrokers	授予获取 MSK 集群中的代理的连接详细信息的权限	读取			
GetClusterPolicy	授予描述集群基于资源的策略的权限	读取	cluster*		
GetCompatibleKafkaVersions	授予获取可将 MSK 集群更新到其中的 Apache Kafka 版本列表的权限	列表			
ListClientVpcConnections	授予列出为某相集群创建的所有 MSK VPC 连接的权限	列表	cluster*		
ListClusterOperations	授予权限以返回已在指定 MSK 集群上执行的所有操作列表	列表	cluster*		
ListClusterOperationsV2	授予权限以返回已在指定 MSK 集群上执行的所有操作列表	List	cluster*		
ListClusters	授予列出此账户中所有 MSK 集群的权限	列表			
ListClustersV2	授予列出此账户中所有 MSK 集群的权限	List			
ListConfigurationRevisions	授予列出此账户中 MSK 配置的所有修订的权限	List	configuration*		
ListConfigurations	授予列出此账户中所有 MSK 配置的权限	List			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListKafkaVersions	授予列出 Amazon MSK 支持的所有 Apache Kafka 版本的权限	List			
ListNodes	授予列出 MSK 集群中代理的权限	列表	cluster*		
ListReplicators	授予权限以列出此账户中所有 MSK 复制程序	列表			
ListScramSecrets	授予列出与 Amazon MSK 集群关联的 Scram 密钥的权限	List	cluster*		
ListTagsForResource	授予列出 MSK 资源的标签的权限	读取	cluster*		
ListVpcConnections	授予列出此账户使用的所有 MSK VPC 连接的权限	列表			
PutClusterPolicy	授予权限以创建或更新集群的基于资源的策略	写入	cluster*		
RebootBroker	授予重启代理的权限	写入	cluster*		
RejectClientVpcConnection	授予拒绝 MSK VPC 连接的权限	写入	cluster* vpc-connection*		
TagResource	授予标记 MSK 资源的权限	Tagging	cluster		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			vpc-connection		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予从 MSK 资源中删除标签的权限	Tagging	cluster		
			vpc-connection		
				aws:TagKeys	
UpdateBrokerCount	授予权限以更新 MSK 集群代理数量	Write	cluster*		
UpdateBrokerStorage	授予权限以更新 MSK 集群代理的存储大小	Write	cluster*		
UpdateBrokerType	授予权限以更新 Amazon MSK 集群的代理类型	Write	cluster*		
UpdateClusterConfiguration	授予更新 MSK 集群配置的权限	Write	cluster*		
			configuration*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateClusterKafkaVersion	授予将 MSK 集群更新到指定 Apache Kafka 版本的权限	Write	cluster*		
UpdateConfiguration	授予创建新修订版 MSK 配置的权限	写入	configuration*		
UpdateConnectivity	授予更新 MSK 集群连接性设置的权限	写入	cluster*		ec2:DescribeRouteTables ec2:DescribeSubnets
				kafka:publicAccessEnabled	
UpdateMonitoring	授予更新 MSK 集群监控设置的权限	写入	cluster*		
UpdateReplicationInfo	授予权限以更新 MSK 复制程序的复制信息	写入	replicator*		
UpdateSecurity	授予更新 MSK 集群安全设置的权限	写入	cluster*		kms:RetireGrant
UpdateStorage	授予更新与 MSK 代理关联的 EBS 存储（大小或预置吞吐量）或将集群存储模式设置为 TIERED 的权限	写入	cluster*		

Amazon Managed Streaming for Apache Kafka 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
cluster	arn:${Partition}:kafka:${Region}:${Account}:cluster/${ClusterName}/${Uuid}	aws:ResourceTag/${TagKey}
configuration	arn:${Partition}:kafka:${Region}:${Account}:configuration/${ConfigurationName}/${Uuid}	
vpc-connection	arn:${Partition}:kafka:${Region}:${VpcOwnerAccount}:vpc-connection/${ClusterOwnerAccount}/${ClusterName}/${Uuid}	aws:ResourceTag/${TagKey}
replicator	arn:${Partition}:kafka:${Region}:${Account}:replicator/${ReplicatorName}/${Uuid}	aws:ResourceTag/${TagKey}
topic	arn:${Partition}:kafka:${Region}:${Account}:topic/${ClusterName}/${ClusterUuid}/${TopicName}	
group	arn:${Partition}:kafka:${Region}:${Account}:group/${ClusterName}/${ClusterUuid}/${GroupName}	
transactional-id	arn:${Partition}:kafka:${Region}:${Account}:transactional-id/${ClusterName}/${ClusterUuid}/${TransactionalId}	

Amazon Managed Streaming for Apache Kafka 的条件键

Amazon Managed Streaming for Apache Kafka 定义以下可以在 IAM policy 的 `Condition` 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对来筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按附加到资源的标签键值对筛选操作	字符串
aws:TagKeys	根据在请求中是否具有标签键来筛选访问	ArrayOfString
kafka:publicAccessEnabled	根据在请求中是否启用了公有访问来筛选访问权限	布尔型

Amazon Managed Workflows for Apache Airflow 的操作、资源和条件键

Amazon Managed Workflows for Apache Airflow（服务前缀：`airflow`）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Managed Workflows for Apache Airflow 定义的操作
- Amazon Managed Workflows for Apache Airflow 定义的资源类型

- Amazon Managed Workflows for Apache Airflow 的条件键

Amazon Managed Workflows for Apache Airflow 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateCliToken	授予创建允许用户通过 Apache Airflow Webserver 上的终端节点调用 Airflow CLI 短期令牌的权限	Write	environment*		
CreateEnvironment	授予创建 Amazon MWAA 环境的权限	Write	environment*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebLoginToken	授予创建允许用户登录 Apache Airflow Web UI 的短期令牌的权限	Write	rbac-role*		
DeleteEnvironment	授予删除 Amazon MWAA 环境的权限	Write	environment*		
				aws:ResourceTag/${TagKey}	
GetEnvironment	授予查看 Amazon MWAA 环境的详细信息的权限	读取	environment*		
				aws:ResourceTag/${TagKey}	
InvokeRestApi	授予权限以通过 Apache Airflow Webserver 上的端点调用 Airflow REST API	写入	rbac-role*		
ListEnvironments	授予列出账户中 Amazon MWAA 环境的权限	List			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListTagsForResource	授予列出 Amazon MWAA 环境标签的权限	Read	environment		
				aws:ResourceTag/${TagKey}	
PublishMetrics	授予发布 Amazon MWAA 环境指标的权限	Write	environment*		
TagResource	授予标记 Amazon MWAA 环境的权限	Tagging	environment		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	授予取消标记 Amazon MWAA 环境的权限	Tagging	environment		
				aws:TagKeys aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateEnvironment	授予修改 Amazon MWAA 环境的权限	Write	environment*		
				aws:ResourceTag/${TagKey}	

Amazon Managed Workflows for Apache Airflow 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
environment	arn:${Partition}:airflow:${Region}:${Account}:environment/${EnvironmentName}	
rbac-role	arn:${Partition}:airflow:${Region}:${Account}:role/${EnvironmentName}/${RoleName}	

Amazon Managed Workflows for Apache Airflow 的条件键

Amazon Managed Workflows for Apache Airflow 定义以下可以在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对来筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按附加到资源的标签键值对筛选操作	字符串
aws:TagKeys	按请求中的标签键筛选访问权限	ArrayOfString

Amazon Web Services Marketplace的操作、资源和条件键

Amazon Web Services Marketplace （服务前缀:aws-marketplace）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Web Services Marketplace定义的操作
- Amazon Web Services Marketplace定义的资源类型
- Amazon Web Services Marketplace的条件键

Amazon Web Services Marketplace定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须

具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AcceptAgreementApprovalRequest	授予用户批准传入订阅请求（针对提供的产品需要订阅验证的提供商）的权限	写入			
AcceptAgreementRequest	授予用户权限，以接受其协议请求。请注意，此操作不适用于 Marketplace 购买	写入			
CancelAgreement	授予用户权限，以取消其协议。请注意，此操作不适用于 Marketplace 购买	写入			
CancelAgreementRequest	授予用户针对需要订阅验证的产品，取消待处理的订阅请求的权限	写入			
CreateAgreementRequest	授予用户权限，以创建协议请求。请注意，此操作不适用于 Marketplace 购买	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeAgreement	授予用户描述协议相关元数据的权限	读取			
GetAgreementApprovalRequest	授予用户查看其传入订阅请求（针对提供的产品需要订阅验证的提供商）的详细信息的权限。	读取			
GetAgreementRequest	授权用户针对需要订阅验证的数据产品，查看其订阅请求的详细信息的权限。	读取			
GetAgreementTerms	授予用户获取协议条款列表的权限	列表			
ListAgreementApprovalRequests	授予用户列出其传入订阅请求（针对提供的产品需要订阅验证的提供商）的权限	列表			
ListAgreementCharges	向用户授予查看与其协议相关的费用的权限	列表			
ListAgreementRequests	授予用户针对需要订阅验证的产品，列出其订阅请求的权限	列表			
ListEntitlementDetails	授予用户查看与协议相关的权利详细信息的权限。请注意，此操作不适用于 Marketplace 购买	读取			
RejectAgreementApprovalRequest	授予用户拒绝传入订阅请求（针对提供的产品需要订阅验证的提供商）的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
SearchAgreements	授予用户搜索其协议的权限	列表			
Subscribe	向用户授予订阅 Amazon Web Services Marketplace 产品的权限。包括为需要订阅验证的产品发送订阅请求的功能。包括为现有订阅启用自动续订的功能	写入			
Unsubscribe	向用户授予删除 Amazon Web Services Marketplace 产品订阅的权限。包括为现有订阅禁用自动续订的功能	写入			
UpdateAgreementApprovalRequest	授予用户对传入的订阅请求进行更改，包括删除潜在订阅者信息的功能（针对提供的产品需要订阅验证的提供商）的权限	写入			
UpdatePurchaseOrders	允许用户更新与其协议相关的费用的采购订单	写入			
ViewSubscriptions	授予用户查看其账户订阅的权限	列表			

Amazon Web Services Marketplace定义的资源类型

Amazon Web Services Marketplace 不支持在 IAM 策略声明的`Resource`元素中指定资源 ARN。要允许对 Amazon Web Services Marketplace的访问权限，请在策略中指定 `"Resource": "*"`。

Amazon Web Services Marketplace的条件键

Amazon Web Services Marketplace 定义了可在 IAM 策略Condition元素中使用的以下条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws-marketplace:AgreementType	按协议的类型筛选访问权限	ArrayOfString
aws-marketplace:PartyType	按协议的参与方类型筛选访问权限	字符串
aws-marketplace:ProductId	按产品编号筛选基岩产品的访问权限。 Amazon Web Services Marketplace RedHat OpenShift 注意：使用此条件键不会限制对以下产品的访问 Amazon Web Services Marketplace	ArrayOfString

Amazon Web Services Marketplace Entitlement Service 的操作、资源和条件键

Amazon Web Services Marketplace 授权服务（服务前缀:aws-marketplace）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Web Services Marketplace Entitlement Service 定义的操作
- Amazon Web Services Marketplace Entitlement Service 定义的资源类型
- Amazon Web Services Marketplace Entitlement Service 的条件键

Amazon Web Services Marketplace Entitlement Service 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetEntitlements	授予权限以检索给定产品权利值。可以根据客户标识符或产品维度来筛选结果	Read			

Amazon Web Services Marketplace Entitlement Service 定义的资源类型

Amazon Web Services Marketplace 授权服务不支持在 IAM 策略声明的`Resource`元素中指定资源 ARN。要允许对 Amazon Web Services Marketplace Entitlement Service 的访问权限，请在策略中指定 `"Resource": "*"`。

Amazon Web Services Marketplace Entitlement Service 的条件键

Marketplace Entitlement 没有可以在策略语句的 Condition 元素中使用的服务特定上下文键。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon Web Services Marketplace Management Portal 的操作、资源和条件键

Amazon Web Services Marketplace 管理门户（服务前缀:aws-marketplace-management）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon Web Services Marketplace Management Portal 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetAdditionalSellerNotificationRecipients[仅权限]	授予查看其他卖家通知收件人的权限	读取			
GetBankAccountVerificationDetails[仅权限]	授予查看银行账户验证状态的权限	读取			
GetSecondaryUserVerificationDetails[仅权限]	授予查看辅助用户账户验证状态的权限	读取			
GetSellerVerificationDetails[仅权限]	授予查看账户验证状态的权限	读取			
PutAdditionalSellerNotifica	授予更新其他卖家通知收件人的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
tionRecipients[仅权限]					
PutBankAccountVerificationDetails[仅权限]	授予更新银行账户验证状态的权限	写入			
PutSecondaryUserVerificationDetails[仅权限]	授予更新辅助用户账户验证状态的权限	写入			
PutSellerVerificationDetails[仅权限]	授予更新账户验证状态的权限	写入			
uploadFiles[仅权限]	允许访问 Amazon Web Services Marketplace 管理门户中的 “文件上传” 页面	写入			
viewMarketing[仅权限]	允许访问 Amazon Web Services Marketplace 管理门户中的 “营销” 页面	列表			
viewReports[仅权限]	允许访问 Amazon Web Services Marketplace 管理门户中的 “报告” 页面	列表			
viewSettings[仅权限]	允许访问 Amazon Web Services Marketplace 管理门户中的 “设置” 页面	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
viewSupport[仅权限]	允许访问 Amazon Web Services Marketplace 管理门户中的 Customer Support 资格页面	列表			

Amazon Web Services Marketplace Management Portal 定义的资源类型

Amazon Web Services Marketplace 管理门户网站不支持在 IAM 策略声明的`Resource`元素中指定资源 ARN。要允许对 Amazon Web Services Marketplace Management Portal 的访问权限，请在策略中指定 `"Resource": "*"`。

Amazon Web Services Marketplace Management Portal 的条件键

Marketplace Portal 没有可以在策略语句的 `Condition` 元素中使用的服务特定上下文键。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon Web Services Marketplace Metering Service 的操作、资源和条件键

Amazon Web Services Marketplace 计量服务（服务前缀:`aws-marketplace`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Web Services Marketplace Metering Service 定义的操作
- Amazon Web Services Marketplace Metering Service 定义的资源类型
- Amazon Web Services Marketplace Metering Service 的条件键

Amazon Web Services Marketplace Metering Service 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchMeterUsage	授予为 SaaS 应用程序发布一组客户的计量记录的权限	Write			
MeterUsage	授予发出计量记录的权限	写入			
RegisterUsage	授予权限以验证运行您的付费软件的客户是否已订阅您的产品 Amazon Web Services Marketplace，从而使您能够防范未经授权的使用。计量每	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
	个 ECS 任务每小时使用软件的情况，以将用量按比例分配到秒。				
ResolveCustomer	授予解析注册令牌以获取 CustomerIdentifier 和产品代码的权限	写入			

Amazon Web Services Marketplace Metering Service 定义的资源类型

Amazon Web Services Marketplace 计量服务不支持在 IAM 策略声明的`Resource`元素中指定资源 ARN。要允许对 Amazon Web Services Marketplace Metering Service 的访问权限，请在策略中指定`"Resource": "*"`。

Amazon Web Services Marketplace Metering Service 的条件键

Marketplace Metering 没有可以在策略语句的 `Condition` 元素中使用的服务特定上下文键。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon MemoryDB 的操作、资源和条件密钥

Amazon MemoryDB（服务前缀：`memorydb`）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon MemoryDB 定义的操作
- Amazon MemoryDB 定义的资源类型

- Amazon MemoryDB 的条件密钥

Amazon MemoryDB 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

> **Note**
>
> 在 IAM 中为 Redis 策略创建 MemoryDB 时，必须为资源块使用 "*" 通配符。有关在 IAM policy 中使用以下 MemoryDB for Redis API 操作的信息，请参阅 MemoryDB 操作和 IAM。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchUpdateCluster	授予应用服务更新的权限	写入	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs s3:GetObject
				aws:ResourceTag/${TagKey}	
Connect	允许 IAM 用户或角色作为指定的 MemoryDB 用户连接到集群中的节点	写入	cluster*		
			user*		
				aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CopySnapshot	授予权限以复制现有快照	写入	snapshot*		memorydb:TagResource s3:DeleteObject s3:GetBucketAcl s3:PutObject
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateAcl	授予权限以创建新的访问控制列表	写入	user*		memorydb:TagResource

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateCluster	授予权限以创建集群	写入	acl*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs memorydb:TagResource s3:GetObject
			parametergroup*		
			subnetgroup*		
			multiregioncluster		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			snapshot		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys memorydb:TLSEnabled	
CreateMultiRegionCluster	授予创建多区域集群的权限	写入	multiregionparametergroup*		memorydb:TagResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys memorydb:TLSEnabled	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateParameterGroup	授予权限以创建新的参数组	写入		aws:RequestTag/${TagKey} aws:TagKeys	memorydb:TagResource
CreateSnapshot	授予在当前时间点创建群集备份的权限	写入	cluster*		memorydb:TagResource s3:DeleteObject s3:GetBucketAcl s3:PutObject
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateSubnetGroup	授予权限以创建新的子网组	写入		aws:RequestTag/${TagKey} aws:TagKeys	memorydb:TagResource
CreateUser	授予权限以创建新用户	写入		aws:RequestTag/${TagKey} aws:TagKeys memorydb:UserAuthenticationMode	memorydb:TagResource
DeleteAcl	授予权限以删除访问控制列表	写入	acl*		
				aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteCluster	授予权限以删除以前预配置的集群	写入	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			multiregioncluster		
			snapshot		
				aws:ResourceTag/${TagKey}	
DeleteMultiRegionCluster	授予删除多区域集群的权限	写入	multiregioncluster*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey}	
DeleteParameterGroup	授予权限以删除参数组	写入	parametergroup*		
				aws:ResourceTag/${TagKey}	
DeleteSnapshot	授予权限以删除快照	写入	snapshot*		
				aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteSubnetGroup	授予删除子网组的权限	写入	subnetgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	
DeleteUser	授予权限，以删除用户	写入	user*		
				aws:ResourceTag/${TagKey}	
DescribeAcls	授予权限以检索有关 IP 访问控制列表的信息	读取	acl*		
				aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeClusters	如果未指定集群标识符，则授予检索有关所有已设置集群的信息的权限；如果提供了集群标识符，则授予检索有关特定集群的信息的权限	读取	cluster*		
				aws:ResourceTag/${TagKey}	
DescribeEngineVersions	授予权限以列出可用的引擎及其版本	读取			
DescribeEvents	授予权限以检索与集群、子网组和参数组相关的事件	读取			
DescribeMultiRegionClusters	如果未指定集群标识符，则授予检索有关所有多区域集群的信息的权限；如果提供了集群标识符，则授予检索有关特定多区域集群的信息的权限	读取	multiregioncluster*		
				aws:ResourceTag/${TagKey}	
DescribeMultiRegionParameterGroups	授予检索有关多区域参数组信息的权限	读取	multiregionparametergroup*		
DescribeMultiRegionParameters	授予检索特定多区域参数组的详细参数列表的权限	读取	multiregionparametergroup*		
DescribeParameterGroups	授予权限以检索有关参数组的信息	读取	parametergroup*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey}	
DescribeParameters	授予权限以检索特定参数组的详细参数列表	读取	parametergroup*		
				aws:ResourceTag/${TagKey}	
DescribeReservedNodes	授予检索预留节点的权限	读取	reservednode*		
				aws:ResourceTag/${TagKey}	
DescribeReservedNodesOfferings	授予检索预留节点产品的权限	读取			
DescribeServiceUpdates	授予权限以检索服务更新详细信息	读取			
DescribeSnapshots	授予权限以检索有关集群快照的信息	读取	snapshot*		
				aws:ResourceTag/${TagKey}	
DescribeSubnetGroups	授予权限以检索子网组列表	读取	subnetgroup*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey}	
DescribeUsers	授予权限以检索有关用户的信息	读取	user*		
				aws:ResourceTag/${TagKey}	
FailoverShard	授予权限以测试集群中的指定分片上的自动故障转移	写入	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListAllowedMultiRegionClusterUpdates	授予列出可用多区域集群更新的权限	读取	multiregioncluster*		
				aws:ResourceTag/${TagKey}	
ListAllowedNodeTypeUpdates	授予列出可用节点类型更新的权限	读取	cluster*		
				aws:ResourceTag/${TagKey}	
ListTags	授予列出成本分配标签的权限	读取	acl		
			cluster		
			multiregioncluster		
			parametergroup		
			snapshot		
			subnetgroup		
			user		
				aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PurchaseReservedNodesOffering	授予购买新预留节点的权限	写入	reservednode*		memorydb:TagResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
ResetParameterGroup	授予权限以将参数组的参数修改为引擎或者系统默认值	写入	parametergroup*		
				aws:ResourceTag/${TagKey}	
TagResource	授予将最多 10 个成本分配标签添加到命名资源的权限	标记	acl		
			cluster		
			multiregioncluster		
			parametergroup		
			reservednode		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			snapshot		
			subnetgroup		
			user		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	授予从资源中移除 TagKeys 列表标识的标签的权限	标记	acl		
			cluster		
			multiregioncluster		
			parametergroup		
			snapshot		
			subnetgroup		
			user		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateAcl	授予更新访问控制规则的权限	写入	acl*		
			user*		
				aws:ResourceTag/${TagKey}	
UpdateCluster	授予更新集群设置的权限	写入	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			acl		
			parameter group		
				aws:ResourceTag/${TagKey}	
UpdateMultiRegionCluster	授予更新多区域集群设置的权限	写入	multiregioncluster *		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			multiregionparametergroup		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey}	
UpdateParameterGroup	授予权限以更新参数组的参数	写入	parametergroup*		
				aws:ResourceTag/${TagKey}	
UpdateSubnetGroup	授予权限以更新子网组	写入	subnetgroup*		
				aws:ResourceTag/${TagKey}	
UpdateUser	授予权限以更新用户	写入	user*		
				aws:ResourceTag/${TagKey} memorydb:UserAuthenticationMode	

Amazon MemoryDB 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从

而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
multiregionparametergroup	arn:${Partition}:memorydb::${Account}:multiregionparametergroup/${MultiRegionParameterGroupName}	
parametergroup	arn:${Partition}:memorydb:${Region}:${Account}:parametergroup/${ParameterGroupName}	aws:ResourceTag/${TagKey}
subnetgroup	arn:${Partition}:memorydb:${Region}:${Account}:subnetgroup/${SubnetGroupName}	aws:ResourceTag/${TagKey}
multiregioncluster	arn:${Partition}:memorydb::${Account}:multiregioncluster/${ClusterName}	aws:ResourceTag/${TagKey} memorydb:TLSEnabled
cluster	arn:${Partition}:memorydb:${Region}:${Account}:cluster/${ClusterName}	aws:ResourceTag/${TagKey}
snapshot	arn:${Partition}:memorydb:${Region}:${Account}:snapshot/${SnapshotName}	aws:ResourceTag/${TagKey}
user	arn:${Partition}:memorydb:${Region}:${Account}:user/${UserName}	aws:ResourceTag/${TagKey}
acl	arn:${Partition}:memorydb:${Region}:${Account}:acl/${AclName}	aws:ResourceTag/${TagKey}
reservednode	arn:${Partition}:memorydb:${Region}:${Account}:reservednode/${ReservationID}	aws:ResourceTag/${TagKey}

Amazon MemoryDB 的条件密钥

Amazon MemoryDB 定义以下可在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中传递的标签筛选操作	字符串
aws:ResourceTag/${TagKey}	根据与资源关联的标签筛选操作	字符串
aws:TagKeys	根据在请求中传递的标签键筛选操作	ArrayOfString
memorydb:TLSEnabled	按请求中存在的 TLSEnabled 参数过滤访问权限，如果参数不存在，则默认为 true 值	布尔型
memorydb:UserAuthenticationMode	按请求中的 UserAuthenticationMode .Type 参数筛选访问权限	字符串

Amazon Message Delivery Service 的操作、资源和条件键

Amazon Message Delivery Service（服务前缀：ec2messages）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Message Delivery Service 定义的操作

- Amazon Message Delivery Service 定义的资源类型
- Amazon Message Delivery Service 的条件键

Amazon Message Delivery Service 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AcknowledgeMessage	授予确认消息，从而确保不会再次发送它的权限	Write			
DeleteMessage	授予删除消息的权限	Write			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
FailMessage	授予权限以使消息失败，表明无法成功处理该消息，从而确保无法回复或再次发送它	Write			
GetEndpoint	授予权限以根据消息的给定目标，将流量路由到正确的终端节点	Read			
GetMessages	授予权限以使用长轮询向客户端/实例发送消息	Read		ssm:SourceInstanceARN ec2:SourceInstanceARN	
SendReply	授予权限以将来自客户端/实例的回复发送到上游服务	Write		ssm:SourceInstanceARN ec2:SourceInstanceARN	

Amazon Message Delivery Service 定义的资源类型

Amazon Message Delivery Service 不支持在 IAM policy 语句的 `Resource` 元素中指定资源 ARN。要允许对 Amazon Message Delivery Service 的访问权限，请在策略中指定 `"Resource": "*"`。

Amazon Message Delivery Service 的条件键

Amazon Message Delivery Service 定义以下可以在 IAM policy 的 `Condition` 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
ec2:SourceInstanceARN	按发起请求的实例的 ARN 筛选访问	ARN
ssm:SourceInstanceARN	通过验证发出请求的 Amazon 系统管理员托管实例的 Amazon 资源名称 (ARN) 来筛选访问权限。当请求来自通过与实例配置文件关联的 IAM 角色进行身份验证的托管实例时，此密钥不存在 EC2	ARN

Amazon Message Gateway Service 的操作、资源和条件键

Amazon Message Gateway Service（服务前缀：ssmmessages）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Message Gateway Service 定义的操作
- Amazon Message Gateway Service 定义的资源类型
- Amazon Message Delivery Service 的条件键

Amazon Message Gateway Service 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须

具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateControlChannel	授予权限以为实例注册控制通道以将控制消息发送到 Systems Manager 服务	Write		ssm:SourceInstanceARN ec2:SourceInstanceARN	
CreateDataChannel	授予权限以为实例注册数据通道以将数据消息发送到 Systems Manager 服务	Write			
OpenControlChannel	授予权限以为注册的控制通道流打开从实例到 Systems Manager 服务的 WebSocket 连接	Write			
OpenDataChannel	授予权限以为注册的数据通道流打开从实例到 Systems	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
	Manager 服务的 WebSocket 连接				

Amazon Message Gateway Service 定义的资源类型

Amazon Message Gateway Service 不支持在 IAM 策略语句的 `Resource` 元素中指定资源 ARN。要允许对 Amazon Message Delivery Service 的访问，请在策略中指定 `"Resource": "*"`。

Amazon Message Delivery Service 的条件键

Amazon Message Delivery Service 定义以下可以在 IAM 策略的 `Condition` 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
ec2:SourceInstanceARN	按发起请求的实例的 ARN 筛选访问	ARN
ssm:SourceInstanceARN	通过验证发出请求的 Amazon 系统管理员托管实例的 Amazon 资源名称 (ARN) 来筛选访问权限。当请求来自通过与实例配置文件关联的 IAM 角色进行身份验证的托管实例时，此密钥不存在 EC2	ARN

Amazon MQ 的操作、资源和条件键

Amazon MQ（服务前缀：`mq`）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。

- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon MQ 定义的操作
- Amazon MQ 定义的资源类型
- Amazon MQ 的条件键

Amazon MQ 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateBroker	授予创建代理的权限	Write		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateSecurityGroup ec2:CreateVpcEndpoint ec2:DescribeInternetGateways ec2:DescribeNetworkInterfacePermissions ec2:DescribeNetworkInterfaces

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
					ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyNetworkInterfaceAttribute iam:CreateServiceLinkedRole route53:AssociateVPCWithHostedZone
CreateConfiguration	授予权限以便为指定的配置名称创建新的配置。Amazon MQ 使用默认配置（引擎类型和引擎版本）	写入		aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateReplicaBroker[仅权限]	授予权限以创建复制代理	写入	brokers*		
CreateTags	授予创建标签的权限	Tagging	brokers		
			configurations		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUser	授予创建 ActiveMQ 用户的权限	Write	brokers*		
DeleteBroker	授予删除代理的权限	Write	brokers*		ec2:DeleteNetworkInterface ec2:DeleteNetworkInterfacePermission ec2:DeleteVpcEndpoints ec2:DetachNetworkInterface

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteTags	授予删除标签的权限	Tagging	brokers		
			configurations		
				aws:TagKeys	
DeleteUser	授予删除 ActiveMQ 用户的权限	Write	brokers*		
DescribeBroker	授予返回指定代理相关信息的权限	Read	brokers*		
DescribeBrokerEngineTypes	授予返回代理引擎相关信息的权限	Read			
DescribeBrokerInstanceOptions	授予权限以返回有关代理实例选项的信息	Read			
DescribeConfiguration	授予返回指定配置相关信息的权限	Read	configurations*		
DescribeConfigurationRevision	授予为指定配置返回指定配置修订的权限	Read	configurations*		
DescribeUser	授予返回 ActiveMQ 用户相关信息的权限	Read	brokers*		
ListBrokers	授予返回所有代理的列表的权限	List			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListConfigurationRevisions	授予为指定配置返回所有现有修订的列表的权限	List	configurations*		
ListConfigurations	授予返回所有配置的列表的权限	List			
ListTags	授予返回标签列表的权限	List	brokers		
			configurations		
ListUsers	授予返回所有 ActiveMQ 用户的列表的权限	列表	brokers*		
Promote	授予权限以提升代理	写入	brokers*		
RebootBroker	授予重新引导代理的权限	Write	brokers*		
UpdateBroker	授予向代理添加待处理的配置更改的权限	Write	brokers*		
UpdateConfiguration	授予更新指定配置的权限	Write	configurations*		
UpdateUser	授予更新 ActiveMQ 用户信息的权限	Write	brokers*		

Amazon MQ 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
brokers	arn:${Partition}:mq:${Region}:${Account}:broker:${BrokerName}:${BrokerId}	aws:ResourceTag/${TagKey}
configurations	arn:${Partition}:mq:${Region}:${Account}:configuration:${ConfigurationId}	aws:ResourceTag/${TagKey}

Amazon MQ 的条件键

Amazon MQ 定义以下可以在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString

Amazon Neptune 的操作、资源和条件键

Amazon Neptune（服务前缀：neptune-db）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。

- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Neptune 定义的操作
- Amazon Neptune 定义的资源类型
- Amazon Neptune 的条件键

Amazon Neptune 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CancelLoaderJob	授予权限以取消加载程序任务	写入	database*		
CancelMLDataProcessingJob	授予权限以取消 ML 数据处理任务	写入	database*		
CancelMLModelTrainingJob	授予权限以取消 ML 模型训练任务	写入	database*		
CancelMLModelTransformJob	授予权限以取消 ML 模型转换任务	写入	database*		
CancelQuery	授予权限以取消查询	写入	database*		
CreateMLEndpoint	授予权限以创建 ML 端点	写入	database*		
DeleteDataViaQuery	授予通过数据库查询 APIs 运行删除数据的权限	写入	database*		
				neptune-db:QueryLanguage	
DeleteMLEndpoint	授予权限以删除 ML 端点	写入	database*		
DeleteStatistics	授予权限以删除数据库中的所有统计数据	写入	database*		
GetEngineStatus	授予权限以检查 Neptune 引擎的状态	读取	database*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetGraphSummary	授予权限以从数据库获取图形摘要	读取	database*		
GetLoaderJobStatus	授予权限以检查加载程序任务的状态	读取	database*		
GetMLDataProcessingJobStatus	授予权限以检查 ML 数据处理任务的状态	读取	database*		
GetMLEndpointStatus	授予权限以检查 ML 端点的状态	读取	database*		
GetMLModelTrainingJobStatus	授予权限以检查 ML 模型训练任务的状态	读取	database*		
GetMLModelTransformJobStatus	授予权限以检查 ML 模型转换任务的状态	读取	database*		
GetQueryStatus	授予权限以检查所有活动查询的状态	读取	database*		
				neptune-db:QueryLanguage	
GetStatisticsStatus	授予权限以检查数据库统计数据的状态	读取	database*		
GetStreamRecords	授予权限以取回来自 Neptune 的流记录	读取	database*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				neptune-db:QueryLanguage	
ListLoaderJobs	授予权限以列出所有加载程序任务	列表	database*		
ListMLDataProcessingJobs	授予权限以列出所有 ML 数据处理任务	列表	database*		
ListMLEndpoints	授予权限以列出所有 ML 端点	列表	database*		
ListMLModelTrainingJobs	授予权限以列出所有 ML 模型训练任务	列表	database*		
ListMLModelTransformJobs	授予权限以列出所有 ML 模型转换任务	列表	database*		
ManageStatistics	授予权限以管理数据库中的统计数据	写入	database*		
ReadDataViaQuery	授予通过数据库查询 APIs 运行读取数据的权限	读取	database*		
				neptune-db:QueryLanguage	
ResetDatabase	授予权限以获取重置所需的令牌，并重置 Neptune 数据库	写入	database*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StartLoaderJob	授予权限以启动加载程序任务	写入	database*		
StartMLDataProcessingJob	授予权限以启动 ML 数据处理任务	写入	database*		
StartMLModelTrainingJob	授予权限以启动 ML 模型训练任务	写入	database*		
StartMLModelTransformJob	授予权限以启动 ML 模型转换任务	写入	database*		
WriteDataViaQuery	授予通过数据库查询 APIs 运行写入数据的权限	写入	database*		
				neptune-db:QueryLanguage	
connect	授予 1.2.0.0 版之前的引擎版本所有数据访问操作的权限	写入	database*		

Amazon Neptune 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
database	arn:${Partition}:neptune-db:${Region}:${Account}:${ClusterResourceId}/*	

Amazon Neptune 的条件键

Amazon Neptune 定义以下可以在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
neptune-db:QueryLanguage	按图表模型筛选访问权限	字符串

Amazon Network Firewall 的操作、资源和条件键

Amazon Network Firewall（服务前缀:network-firewall）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Network Firewall 定义的操作
- Amazon Network Firewall 定义的资源类型
- Amazon Network Firewall 的条件键

Amazon Network Firewall 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateFirewallPolicy	授予在防火墙策略和防火墙之间创建关联的权限	Write	Firewall*		
			FirewallPolicy*		
AssociateSubnets	授予将 VPC 子网关联到防火墙的权限	写入	Firewall*		
CreateFirewall	授予创建 Network Fire Amazon wall 防火墙的权限	写入	Firewall*		iam:CreateServiceL

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
					inkedRole
			FirewallPolicy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFirewallPolicy	授予创建 Network Firewall 防火墙策略的权限	写入	FirewallPolicy*		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleGroup	授予创建 Amazon Network Firewall 规则组的权限	写入	StatefulRuleGroup		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			StatelessRuleGroup		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTLSInspectionConfiguration	授予创建 Amazon Network Firewall tls 检查配置的权限	写入	TLSInspectionConfiguration*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFirewall	授予删除防火墙的权限	Write	Firewall*		
DeleteFirewallPolicy	授予删除防火墙策略的权限	Write	FirewallPolicy*		
DeleteResourcePolicy	授予删除防火墙策略或规则组的资源策略的权限	Write	FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteRuleGroup	授予删除规则组的权限	写入	StatefulRuleGroup*		
			StatelessRuleGroup*		
DeleteTLSInspectionConfiguration	授予删除 TLS 检查配置的权限	写入	TLSInspectionConfiguration*		
DescribeFirewall	授予检索定义防火墙的数据对象的权限	Read	Firewall*		
DescribeFirewallPolicy	授予检索定义防火墙策略的数据对象的权限	Read	FirewallPolicy*		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
DescribeLoggingConfiguration	授予描述防火墙日志记录配置的权限	Read	Firewall*		logs:GetLogDelivery logs:ListLogDeliveries

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeResourcePolicy	授予描述防火墙策略或规则组的资源策略的权限	Read	FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		
DescribeRuleGroup	授予检索定义规则组的数据对象的权限	读取	StatefulRuleGroup		
			StatelessRuleGroup		
DescribeRuleGroupMetadata	授予权限以检索规则组的高级信息。	读取	StatefulRuleGroup		
			StatelessRuleGroup		
DescribeTLSInspectionConfiguration	授予检索定义 TLS 检查配置的数据对象的权限	读取	TLSInspectionConfiguration*		
DisassociateSubnets	授予取消 VPC 子网与防火墙的关联的权限	写入	Firewall*		
GetAnalysisReportResults	授予检索防火墙分析报告结果的权限	读取	Firewall*		
ListAnalysisReports	授予列出防火墙分析报告的权限	列表	Firewall*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListFirewallPolicies	授予检索防火墙策略元数据的权限	List	FirewallPolicy*		
ListFirewalls	授予检索防火墙元数据的权限	List	Firewall*		
ListRuleGroups	授予检索规则组元数据的权限	列表			
ListTLSInspectionConfigurations	授予检索 TLS 检查配置的元数据的权限	列表	TLSInspectionConfiguration*		
ListTagsForResource	授予检索资源标签的权限	List	Firewall*		
			FirewallPolicy*		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
PutResourcePolicy	授予为防火墙策略或规则组放置资源策略的权限	写入	FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StartAnalysisReport	授予在防火墙上启动分析报告的权限	写入	Firewall*		
TagResource	授予将标签附加到资源的权限	Tagging	Firewall		
			FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予权限以从资源中删除标签	标记	Firewall		
			FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			TLSInspectionConfiguration		
				aws:TagKeys	
UpdateFirewallAnalysisSettings	授予修改防火墙防火墙分析设置的权限	写入	Firewall*		
UpdateFirewallDeleteProtection	授予添加或删除防火墙的删除保护的权限	Write	Firewall*		
UpdateFirewallDescription	授予修改防火墙描述的权限	写入	Firewall*		
UpdateFirewallEncryptionConfiguration	授予修改防火墙加密配置的权限	写入	Firewall*		
UpdateFirewallPolicy	授予修改防火墙策略的权限	Write	FirewallPolicy*		
			StatefulRuleGroup		
			StatelessRuleGroup		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			TLSInspectionConfiguration		
UpdateFirewallPolicyChangeProtection	授予为防火墙添加或删除防火墙策略更改保护的权限	Write	Firewall*		
UpdateLoggingConfiguration	授予修改防火墙日志记录配置的权限	Write	Firewall*		
UpdateRuleGroup	授予修改规则组的权限	Write	StatefulRuleGroup		
			StatelessRuleGroup		
UpdateSubnetChangeProtection	授予为防火墙添加或删除子网更改保护的权限	写入	Firewall*		
UpdateTLSInspectionConfiguration	授予修改 TLS 检查配置的权限	写入	TLSInspectionConfiguration*		

Amazon Network Firewall 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}

Amazon Network Firewall 的条件键

Amazon Network Firewall 定义了以下可以在 IAM 策略Condition元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按每个标签的允许值集筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签值筛选访问权限	字符串
aws:TagKeys	按请求中是否具有必需标签来筛选访问	ArrayOfString

Amazon OpenSearch 服务的操作、资源和条件密钥

Amazon Service（ OpenSearch 服务前缀:es ）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

亚马逊 OpenSearch 服务定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AcceptInboundConnection	授予目标域拥有者接受入站跨集群搜索连接请求的权限	写入			
AcceptInboundCrossClusterSearchConnection	授予目标域拥有者权限以接受入站跨集群搜索连接请求。此权限已弃用。 AcceptInboundConnection 改用	写入			
AddDataSource	授予为 OpenSearch 服务域添加数据源的权限	写入	domain*		
AddDirectQueryDataSource	授予为所提供的 OpenSearch arn 添加数据源的权限	写入	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
AddTags	授予将资源标签附加到 OpenSearch 服务域、数据源或应用程序的权限	标记	application*		
			datasource*		
			domain*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
AssociatePackage	授予将包与 OpenSearch 服务域关联的权限	写入	domain*		
AssociatePackages	授予将多个包与 OpenSearch 服务域关联的权限	写入	domain*		
AuthorizeVpcEndpointAccess	授予通过使用接口 VPC 终端节点提供对亚马逊 OpenSearch 服务域的访问权限	写入			
CancelDomainConfigChange	授予取消 OpenSearch 服务域变更的权限	写入	domain*		
CancelElasticsearchServiceSoftwareUpdate	授予权限以取消域的服务软件更新。此权限已弃用。CancelServiceSoftwareUpdate 改用	写入	domain*		
CancelServiceSoftwareUpdate	授予权限以取消域的服务软件更新	写入	domain*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateApplication	授予创建 OpenSearch 应用程序的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDomain	授予创建 Amazon OpenSearch 服务域名的权限	写入	domain		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateElasticsearchDomain	授予创建 OpenSearch 服务域的权限。此权限已弃用。CreateDomain 改用	写入	domain		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateElasticsearchServiceRole	授予创建使用 VPC 访问权限的 OpenSearch 服务域所需的服务相关角色的权限。此权限已被弃用。 OpenSearch 服务为您创建服务相关角色	写入			
CreateOutboundConnection	授予新建从源域到目标域的跨集群搜索连接的权限	写入	domain*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateOutboundCrossClusterSearchConnection	授予权限以新建从源域到目标域的跨集群搜索连接。此权限已弃用。 CreateOutboundConnection 改用	写入	domain*		
CreatePackage	授予添加用于 OpenSearch 服务域的软件包的权限	写入			
CreateServiceRole	授予创建使用 VPC 访问权限的 Amazon OpenSearch 服务域所需的服务相关角色的权限	写入			
CreateVpcEndpoint	授予创建亚马逊 OpenSearch 服务托管的 VPC 终端节点的权限	写入			
DeleteApplication	授予删除 OpenSearch 应用程序的权限	写入	application*		
DeleteDataSource	授予删除 OpenSearch 服务域数据源的权限	写入	domain*		
DeleteDirectQueryDataSource	授予删除所提供的 OpenSearch arn 的数据源的权限	写入	datasource*		
DeleteDomain	授予删除亚马逊 OpenSearch 服务域名及其所有数据的权限	写入	domain*		
DeleteElasticsearchDomain	授予删除 OpenSearch 服务域及其所有数据的权限。此权限已弃用。 DeleteDomain 改用	写入	domain*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteElasticsearchServiceRole	授予删除使用 VPC 访问权限的 OpenSearch 服务域所需的服务相关角色的权限。此权限已弃用。您可以使用 IAM API 删除服务相关角色	写入			
DeleteInboundConnection	授予目标域拥有者删除现有入站跨集群搜索连接的权限	写入			
DeleteInboundCrossClusterSearchConnection	授予目标域拥有者权限以删除现有入站跨集群搜索连接。此权限已弃用。 DeleteInboundConnection 改用	写入			
DeleteOutboundConnection	授予源域拥有者删除现有出站跨集群搜索连接的权限	写入			
DeleteOutboundCrossClusterSearchConnection	授予源域拥有者权限以删除现有出站跨集群搜索连接。此权限已弃用。 DeleteOutboundConnection 改用	写入			
DeletePackage	授予从 OpenSearch 服务中删除包裹的权限。程序包不能与任何域关联	写入			
DeleteVpcEndpoint	授予删除亚马逊 OpenSearch 服务托管接口 VPC 终端节点的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeDomain	授予权限以查看指定 OpenSearch 服务域的域配置描述，包括域 ID、服务端点和 ARN	读取	domain*		
DescribeDomainAutoTunes	授予权限以查看指定 OpenSearch 服务域的域的自动调整配置，包括自动调整状态和维护计划	读取	domain*		
DescribeDomainChangeProgress	授予查看 OpenSearch 服务域详情阶段进度的权限	读取	domain*		
DescribeDomainConfig	授予查看 OpenSearch 服务域配置选项和状态描述的权限	读取	domain*		
DescribeDomainHealth	授予权限以查看有关以下方面的信息：域和节点运行状况、备用可用区、每个可用区的节点数以及每个节点的分片数量	读取	domain*		
DescribeDomainNodes	授予权限以查看为域及其配置（包括节点 ID、节点类型、节点状态、可用区、实例类型和存储）创建的节点的相关信息	读取	domain*		
DescribeDomains	授予查看最多五个指定 OpenSearch 服务域的域配置描述的权限	列表	domain*		
DescribeDryRunProgress	授予描述 OpenSearch 服务域更新前验证检查状态的权限	读取	domain*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeElasticsearchDomain	授予权限以查看指定 OpenSearch 服务域的域配置描述，包括域 ID、服务端点和 ARN。此权限已弃用。DescribeDomain 改用	读取	domain*		
DescribeElasticsearchDomainConfig	授予查看 OpenSearch 服务域配置和状态描述的权限。此权限已弃用。 DescribeDomainConfig 改用	读取	domain*		
DescribeElasticsearchDomains	授予查看最多五个指定 Amazon OpenSearch 域名的域名配置描述的权限。此权限已弃用。 DescribeDomains 改用	列表	domain*		
DescribeElasticsearchInstanceTypeLimits	授予查看给定 OpenSearch 版本和实例类型的实例数量、存储空间和主节点限制的权限。此权限已弃用。 DescribeInstanceTypeLimits 改用	列表			
DescribeInboundConnections	授予列出目标域的所有入站跨集群搜索连接的权限	列表			
DescribeInboundCrossClusterSearchConnections	授予权限以列出目标域的所有入站跨集群搜索连接。此权限已弃用。 DescribeInboundConnections 改用	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeInstanceTypeLimits	授予权限以查看给定引擎版本和实例类型的实例计数、存储和主节点 (master node) 限制	列表			
DescribeOutboundConnections	授予列出源域的所有出站跨集群搜索连接的权限	列表			
DescribeOutboundCrossClusterSearchConnections	授予权限以列出源域的所有出站跨集群搜索连接。此权限已弃用。 DescribeOutboundConnections 改用	列表			
DescribePackages	授予描述 OpenSearch 服务域可用的所有软件包的权限	读取			
DescribeReservedElasticsearchInstanceOfferings	授予获取 Amazon OpenSearch 服务的预留实例产品的权限。此权限已弃用。 DescribeReservedInstanceOfferings 改用	列表			
DescribeReservedElasticsearchInstances	授予获取已购买的 OpenSearch 服务预留实例的权限。此权限已弃用。 DescribeReservedInstances 改用	列表			
DescribeReservedInstanceOfferings	授予获取 OpenSearch 服务预留实例产品的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeReservedInstances	授予获取已购买的 OpenSearch 服务预留实例的权限	列表			
DescribeVpcEndpoints	授予描述一个或多个 Amazon OpenSearch 服务托管 VPC 终端节点的权限	列表			
DissociatePackage	授予将包与指定 OpenSearch 服务域解除关联的权限	写入	domain*		
DissociatePackages	授予将多个包与指定 OpenSearch 服务域解除关联的权限	写入	domain*		
ESCrossClusterGet	授予权限以向目标域发送跨集群请求	读取	domain		
ESHttpDelete	授予向发送 HTTP 删除请求的权限 OpenSearch APIs	写入	domain		
ESHttpGet	授予向发送 HTTP GET 请求的权限 OpenSearch APIs	读取	domain		
ESHttpHead	授予向发送 HTTP HEAD 请求的权限 OpenSearch APIs	读取	domain		
ESHttpPatch	授予向发送 HTTP 补丁请求的权限 OpenSearch APIs	写入	domain		
ESHttpPost	授予向发送 HTTP POST 请求的权限 OpenSearch APIs	写入	domain		
ESHttpPut	授予向发送 HTTP PUT 请求的权限 OpenSearch APIs	写入	domain		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetApplication	授予获取有关 OpenSearch 应用程序信息的权限	读取	application*		
GetCompatibleElasticsearchVersions	授予获取可将 OpenSearch 服务域升级到的兼容版本 OpenSearch 和 Elasticsearch 版本列表的权限。此权限已弃用。 GetCompatibleVersions 改用	列表	domain*		
GetCompatibleVersions	授予获取可升级 OpenSearch 服务域的兼容引擎版本列表的权限	列表	domain*		
GetDataSource	授予获取 OpenSearch 服务域数据源的权限	读取	domain*		
GetDirectQueryDataSource	授予获取所提供的 OpenSearch arn 的数据源的权限	读取	datasource*		
GetDomainMaintenanceStatus	授予权限以检索节点的维护操作状态	读取	domain*		
GetPackageVersionHistory	授予获取软件包版本历史记录的权限	读取			
GetUpgradeHistory	授予获取给定 OpenSearch 服务域升级历史记录的权限	读取	domain*		
GetUpgradeStatus	授予获取给定 OpenSearch 服务域升级状态的权限	读取	domain*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListApplications	授予列出 OpenSearch 应用程序的权限	列表	application*		
ListDataSources	授予检索 OpenSearch 服务域数据源列表的权限	列表	domain*		
ListDirectQueryDataSources	授予权限以检索所提供的 OpenSearch arn 的数据源列表	列表	datasource*		
ListDomainMaintenances	授予检索 OpenSearch 服务域维护操作列表的权限	列表	domain*		
ListDomainNames	授予显示当前用户拥有的所有 OpenSearch 服务域名的权限	列表			
ListDomainsForPackage	授予列出与软件包关联的所有 OpenSearch 服务域的权限	列表			
ListElasticsearchInstanceTypeDetails	授予列出给定 OpenSearch 版本的所有实例类型和可用功能的权限。此权限已弃用。ListInstanceTypeDetails 改用	列表			
ListElasticsearchInstanceTypes	授予列出给定 OpenSearch 版本支持的所有 EC2 实例类型的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListElasticsearchVersions	授予在 Amazon OpenSearch 服务上列出所有受支持 OpenSearch 版本的权限。此权限已弃用。 ListVersions 改用	列表			
ListInstanceTypeDetails	授予列出给定版本 OpenSearch 或 Elasticsearch 版本的所有实例类型和可用功能的权限	列表			
ListPackagesForDomain	授予列出与 OpenSearch 服务域关联的所有软件包的权限	列表	domain*		
ListScheduledActions	授予权限以检索为 OpenSearch 服务域安排的配置更改列表	列表	domain*		
ListTags	授予显示 OpenSearch 服务域、数据源或应用程序的所有资源标签的权限	读取	application*		
			datasource*		
			domain*		
ListVersions	授予在亚马逊服务中列出所有支持的版本 OpenSearch 和 Elasticsearch 版本的权限 OpenSearch	列表			
ListVpcEndpointAccess	授予权限以检索有关允许通过使用接口 VPC 终端节点访问给定 Amazon Serv OpenSearch ice 域的每位 Amazon 委托人的信息	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListVpcEndpoints	授予在当前 Amazon Web Services 账户 和地区检索所有 Amazon OpenSearch Service 托管 VPC 终端节点的权限	列表			
ListVpcEndpointsForDomain	授予权限以检索与特定域关联的所有 Ama OpenSearch zon Service 托管 VPC 终端节点	列表			
PurchaseReservedElasticsearchInstanceOffering	授予购买 OpenSearch 服务预留实例的权限。此权限已弃用。 PurchaseReservedInstanceOffering 改用	写入			
PurchaseReservedInstanceOffering	授予购买 OpenSearch 预留实例的权限	写入			
RejectInboundConnection	授予目标域拥有者拒绝入站跨集群搜索连接请求的权限	写入			
RejectInboundCrossClusterSearchConnection	授予目标域拥有者权限以拒绝入站跨集群搜索连接请求。此权限已弃用。 RejectInboundConnection 改用	写入			
RemoveTags	授予从 OpenSearch 服务域、数据源或应用程序中移除资源标签的权限	标记	application*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			datasource*		
			domain*		
				aws:TagKeys	
RevokeVpcEndpointAccess	授予撤销通过接口 VPC 终端节点提供的亚马逊 OpenSearch 服务域访问权限的权限	写入			
StartDomainMaintenance	授予权限以启动节点维护操作	写入	domain*		
StartElasticsearchServiceSoftwareUpdate	授予权限以开启域的服务软件更新。此权限已弃用。StartServiceSoftwareUpdate 改用	写入	domain*		
StartServiceSoftwareUpdate	授予权限以开启域的服务软件更新	写入	domain*		
UpdateApplication	授予更新 OpenSearch 应用程序的权限	写入	application*		
UpdateDataSource	授予更新 OpenSearch 服务域数据源的权限	写入	domain*		
UpdateDirectQueryDataSource	授予更新所提供的 OpenSearch arn 的数据源的权限	写入	datasource*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateDomainConfig	授予修改 OpenSearch 服务域配置的权限，例如实例类型或实例数量	写入	domain*		
UpdateElasticsearchDomainConfig	授予修改 OpenSearch 服务域配置的权限，例如实例类型或实例数量。此权限已弃用。UpdateDomainConfig 改用	写入	domain*		
UpdatePackage	授予更新软件包以用于 OpenSearch 服务域的权限	写入			
UpdatePackageScope	授予更新软件包范围的权限	写入			
UpdateScheduledAction	授予在以后重新安排计划中的 OpenSearch 服务域配置更改的权限	写入	domain*		
UpdateVpcEndpoint	授予修改亚马逊 OpenSearch 服务托管接口 VPC 终端节点的权限	写入			
UpgradeDomain	授予权限以启动将 OpenSearch 服务域升级到给定版本	写入	domain*		
UpgradeElasticsearchDomain	授予启动将 OpenSearch 服务域升级到指定版本的权限。此权限已弃用。 UpgradeDomain 改用	写入	domain*		

由 Amazon OpenSearch 服务定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}

Amazon OpenSearch 服务的条件密钥

Amazon S OpenSearch ervice 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素中。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中传递的标签筛选访问	字符串
aws:ResourceTag/${TagKey}	根据与资源关联的标签筛选访问	字符串
aws:TagKeys	根据在请求中传递的标签键筛选访问	ArrayOfString

Amazon Organizations 的操作、资源和条件键

Amazon Organizations（服务前缀:`organizations`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Organizations 定义的操作
- Amazon Organizations 定义的资源类型
- Amazon Organizations 的条件键

Amazon Organizations 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须

具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AcceptHandshake	授予权限，向握手发起方发送响应，同意握手请求建议的操作	写入	handshake*		iam:CreateServiceLinkedRole
AttachPolicy	授予权限，将策略附加到根、组织单位或单个账户	写入	policy*		
			account		
			organizationalunit		
			root		
				organizations:PolicyType	
CancelHandshake	授予权限，取消握手	写入	handshake*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CloseAccount	授予关闭现在属于组织（O Amazon Web Services 账户 rganizations）一部分的权限，无论是在组织内创建的，还是受邀加入该组织的	写入	account*		
CreateAccount	授予创建自动成为 Amazon Web Services 账户 组织成员的权限，该成员具有发出请求的凭据	写入		aws:RequestTag/${TagKey} aws:TagKeys	
CreateGovCloudAccount	授予创建 Amazon GovCloud（美国）账户的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOrganization	授予创建组织的权限。拥有调用该 CreateOrganization 操作的凭据的账户自动成为新组织的管理账户	写入			iam:CreateServiceLinkedRole
CreateOrganizationalUnit	授予权限，在根或父级组织单位 (OU) 中创建 OU	写入	organizationalunit root		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePolicy	授予创建策略的权限，您可以将其附加到根、组织单位 (OU) 或个人 Amazon Web Services 账户	写入		organizations:PolicyType aws:RequestTag/${TagKey} aws:TagKeys	
DeclineHandshake	授予拒绝握手请求的权限。它会将握手状态设为 DECLINED，有效地停用请求	写入	handshake*		
DeleteOrganization	授予删除组织的权限	写入			
DeleteOrganizationalUnit	授予权限，从根或另一 OU 删除组织单位	写入	organizationalunit*		
DeletePolicy	授予权限，删除您的组织的策略	写入	policy*		
				organizations:PolicyType	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteResourcePolicy	授予删除您的组织的资源策略的权限	写入			
DeregisterDelegatedAdministrator	授予取消将指定成员注册 Amazon Web Services 账户 为由指定的 Amazon 服务的委托管理员的权限 ServicePrincipal	写入	account*		
				organizations:ServicePrincipal	
DescribeAccount	授予权限，检索特定账户与企业相关的详情	读取	account*		
DescribeCreateAccountStatus	授予权限，检索创建账户的异步请求的最新状态	读取			
DescribeEffectivePolicy	授予权限以检索账户的有效策略	读取	account*		
				organizations:PolicyType	
DescribeHandshake	授予权限，检索上次握手请求的详细信息	读取	handshake*		
DescribeOrganization	授予权限，检索调用凭证所属组织的详细信息	读取			
DescribeOrganizationalUnit	授予权限，检索组织单位 (OU) 的相关详情	读取	organizationalunit*		
DescribePolicy	授予权限，检索有关策略的详情	读取	policy*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				organizations:PolicyType	
DescribeResourcePolicy	授予检索资源策略信息的权限	读取			
DetachPolicy	授予权限，将策略从目标根、组织单位或账户分离	写入	policy*		
			account		
			organizationalunit		
			root		
				organizations:PolicyType	
DisableAWSServiceAccess	授予禁用 Amazon 服务（由指定的服务 ServicePrincipal）与 Organizations 集成的 Amazon 权限	写入		organizations:ServicePrincipal	
DisablePolicyType	授予权限，禁用根中的组织策略类型	写入	root*		
				organizations:PolicyType	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
EnableAWSServiceAccess	授予允许将 Amazon 服务（由指定的服务 ServicePrincipal）与 Organizations 集成的 Amazon 权限	写入		organizations:ServicePrincipal	
EnableAllFeatures	授予权限，开始启用组织中所有功能的过程。升级仅支持整合账单功能的组织	写入			
EnablePolicyType	授予权限，启用根中的策略类型	写入	root*		
				organizations:PolicyType	
InviteAccountToOrganization	授予向其他人发送邀请的权限 Amazon Web Services 账户，要求其以成员账户身份加入您的组织	写入	account		
				aws:RequestTag/${TagKey} aws:TagKeys	
LeaveOrganization	授予权限，将成员账户从其父组织中移除	写入			
ListAWSServiceAccessForOrganization	授予权限以检索您为其启用了与组织集成的 Amazon 服务列表	列表			
ListAccounts	授予权限，列出组织中的所有账户	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListAccountsForParent	授予权限，列出组织中包含于根或组织单位 (OU) 之中的账户列表	列表	organizationalunit		
			root		
ListChildren	授予列出父 OU OUs 或根目录中包含的所有或账户的权限	列表	organizationalunit		
			root		
ListCreateAccountStatus	授予权限，列出组织当前跟踪的账户创建异步请求	列表			
ListDelegatedAdministrators	授予列出该组织中指定为授权管理员的 Amazon 账户的权限	列表		organizations:ServicePrincipal	
ListDelegatedServicesForAccount	授予列出该组织中指定账户作为委托管理员的 Amazon 服务的权限	列表	account*		
ListHandshakesForAccount	授予权限，列出与某一账户关联的所有握手	列表			
ListHandshakesForOrganization	授予权限，列出与组织关联的握手	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListOrganizationalUnitsForParent	授予列出上级组织单位或根目录中的所有组织单位 (OUs) 的权限	列表	organizationalunit		
			root		
ListParents	授予列出作为子组织单位或账户直系父级的根单位或组织单位 (OUs) 的权限	列表	account		
			organizationalunit		
ListPolicies	授予权限，列出组织中的所有策略	列表		organizations:PolicyType	
ListPoliciesForTarget	授予权限，列出直接附加到根、组织单位 (OU) 或账户的所有策略	列表	account		
			organizationalunit		
			root		
				organizations:PolicyType	
ListRoots	授予权限，列出组织中定义的所有根	列表			
ListTagsForResource	授予权限以列出指定资源的所有标签	列表	account		
			organizationalunit		
			policy		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			resourcepolicy		
			root		
ListTargetsForPolicy	授予列出所有关联策略的根和账户的权限 OUs	列表	policy*		
				organizations:PolicyType	
MoveAccount	授予权限，将账户从其当前的根或 OU 移动至另一父级根或 OU	写入	account*		
			organizationalunit*		
			root*		
PutResourcePolicy	授予权限以创建或更新资源策略	写入	resourcepolicy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RegisterDelegatedAdministrator	授予注册指定成员账户的权限，以管理由指定的 Amazon 服务的 Organizations 功能 ServicePrincipal	写入	account*		
				organizations:ServicePrincipal	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
RemoveAccountFromOrganization	授予权限，从组织中移除指定账户	写入	account*		
TagResource	授予将一个或多个标签添加到指定资源的权限	Tagging	account		
			organizationalunit		
			policy		
			resourcepolicy		
			root		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	授予从指定资源中删除一个或多个标签的权限	标记	account		
			organizationalunit		
			policy		
			resourcepolicy		
			root		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys	
UpdateOrganizationalUnit	授予权限，将组织单位 (OU) 重命名	写入	organizationalunit*		
UpdatePolicy	授予权限，使用新的名称、描述或内容更新现有策略	写入	policy*		
				organizations:PolicyType	

Amazon Organizations 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}	

资源类型	ARN	条件键
organizationalunit	arn:${Partition}:organizations::${Account}:ou/o-${OrganizationId}/ou-${OrganizationalUnitId}	aws:ResourceTag/${TagKey}
policy	arn:${Partition}:organizations::${Account}:policy/o-${OrganizationId}/${PolicyType}/p-${PolicyId}	aws:ResourceTag/${TagKey}
resourcepolicy	arn:${Partition}:organizations::${Account}:resourcepolicy/o-${OrganizationId}/rp-${ResourcePolicyId}	aws:ResourceTag/${TagKey}
awspolicy	arn:${Partition}:organizations::aws:policy/${PolicyType}/p-${PolicyId}	
root	arn:${Partition}:organizations::${Account}:root/o-${OrganizationId}/r-${RootId}	aws:ResourceTag/${TagKey}

Amazon Organizations 的条件键

Amazon Organizations 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素中。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString

条件键	描述	类型
organizations:PolicyType	按指定的策略类型名称筛选访问	字符串
organizations:ServicePrincipal	按指定的服务主体名称筛选访问	字符串

Amazon Payments 的操作、资源和条件键

Amazon Payments（服务前缀:payments）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Payments 定义的操作
- Amazon Payments 定义的资源类型
- Amazon Payments 的条件键

Amazon Payments 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用

Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AcceptFinancingApplicationTerms	允许接受贷款人提供的融资申请条款	写入			
CreateFinancingApplication	授予创建融资应用程序的权限	写入			
CreatePaymentInstrument	授予创建付款方式的权限	写入		aws:TagKeys aws:RequestTag/${TagKey}	
DeletePaymentInstrument[仅权限]	授予删除付款方式的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetFinancingApplication	授予获取有关融资申请信息的权限	读取			
GetFinancingLine	授予获取有关融资额度的信息的权限	读取			
GetFinancingLineWithdrawal	授予获取有关融资额度提款信息的权限	读取			
GetFinancingOption	授予获取有关融资选项信息的权限	读取			
GetPaymentInstrument	授予获取付款方式信息的权限	列表	payment-instrument		
GetPaymentStatus[仅权限]	授予获取发票付款状态的权限	读取			
ListFinancingApplications	授予列出融资应用程序元数据的权限	列表			
ListFinancingLineWithdrawals	授予列出融资额度提款元数据的权限	列表			
ListFinancingLines	授予列出融资额度元数据的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListPaymentInstruments[仅权限]	授予权限以列出付款工具元数据	列表			
ListPaymentPreferences[仅权限]	授予获取付款偏好（首选付款币种、首选付款方式等）的权限	列表			
ListPaymentProgramOptions	授予列出有关付款选项信息的权限	列表			
ListPaymentProgramStatus	授予列出有关付款计划资格和注册状态信息的权限	列表			
ListTagsForResource	授予权限以列出付款资源的标签	列表	payment-instrument		
MakePayment[仅权限]	授予进行付款、验证付款、验证付款方式，以及为 Advance Pay 生成资金请求文档的权限	写入			
TagResource	授予权限以标记付款资源	标记	payment-instrument		
				aws:TagKeys aws:RequestTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UntagResource	授予权限以取消标记付款资源	标记	payment-instrument		
				aws:TagKeys	
UpdateFinancingApplication	授予更新融资申请的权限	写入			
UpdatePaymentInstrument[仅权限]	授予权限以更新付款工具	写入			
UpdatePaymentPreferences[仅权限]	授予更新付款偏好（首选付款货币、首选付款方式等）的权限	写入			

Amazon Payments 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
payment-instrument	arn:${Partition}:payments::${Account}:payment-instrument:${ResourceId}	aws:ResourceTag/${TagKey}

Amazon Payments 的条件键

Amazon Payments 定义了以下条件密钥，这些条件密钥可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString

Amazon Performance Insights 的操作、资源和条件键

Amazon Performance Insights（服务前缀:pi）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Performance Insights 定义的操作
- Amazon Performance Insights 定义的资源类型
- Amazon Performance Insights 的条件键

Amazon Performance Insights 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreatePerformanceAnalysisReport	授予调用 CreatePerformanceAnalysisReport API 为指定数据库实例创建性能分析报告的权限	写入	perf-reports-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeletePerformanceAnalysisReport	授予调用 DeletePerformanceAnalysisReport API 删除指定数据库实例的性能分析报告的权限	写入	perf-reports-resource*		
DescribeDimensionKeys	授予调用 DescribeDimensionKeys API 以检索特定时间段内某个指标的前 N 个维度密钥的权限	读取	metric-resource*		
				pi:Dimensions	
GetDimensionKeyDetails	授予调用 GetDimensionKeyDetails API 检索指定维度组属性的权限	读取	metric-resource*		
				pi:Dimensions	
GetPerformanceAnalysisReport	授予调用 GetPerformanceAnalysisReport API 以检索指定数据库实例的性能分析报告的权限	读取	perf-reports-resource*		
GetResourceMetadata	授予调用 GetResourceMetadata API 以检索不同功能的元数据的权限	读取	metric-resource*		
GetResourceMetrics	授予在一段时间内调用 GetResourceMetrics API 来检索一组数据源的 PI 指标的权限	读取	metric-resource*		
				pi:Dimensions	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListAvailableResourceDimensions	授予调用 ListAvailableResourceDimensions API 以检索可在指定数据库实例上针对每种指定指标类型查询的维度的权限	读取	metric-resource*		
ListAvailableResourceMetrics	授予调用 ListAvailableResourceMetrics API 以检索可为指定数据库实例查询的指定类型的指标的权限	读取	metric-resource*		
ListPerformanceAnalysisReports	授予调用 ListPerformanceAnalysisReports API 列出指定数据库实例的性能分析报告的权限	列表	perf-reports-resource*		
ListTagsForResource	授予调用 ListTagsForResource API 列出资源标签的权限	列表	perf-reports-resource*		
TagResource	授予调用 TagResource API 为资源添加标签的权限	标记	perf-reports-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予调用 UntagResource API 取消资源标签的权限	标记	perf-reports-resource*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys	

Amazon Performance Insights 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}

Amazon Performance Insights 的条件键

Amazon Performance Insights 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串

条件键	描述	类型
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString
pi:Dimensions	按请求的维度筛选访问权限	ArrayOfString

Amazon Personalize 的操作、资源和条件键

Amazon Personalize（服务前缀：`personalize`）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Personalize 定义的操作
- Amazon Personalize 定义的资源类型
- Amazon Personalize 的条件键

Amazon Personalize 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用

Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateBatchInferenceJob	授予创建批量推理作业的权限	写入	batchInferenceJob*		
CreateBatchSegmentJob	授予创建批量分段任务的权限	写入	batchSegmentJob*		
CreateCampaign	授予创建活动的权限	写入	campaign*		
CreateDataDeletionJob	授予权限以创建数据删除作业	写入	dataDeletionJob*		
CreateDataInsightsJob	授予权限以创建数据洞察任务	写入	dataInsightsJob*		
CreateDataset	授予创建数据集的权限	写入	dataset*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateDatasetExportJob	授予创建数据集导出作业的权限	写入	datasetExportJob*		
CreateDatasetGroup	授予创建数据集组的权限	Write	datasetGroup*		
CreateDatasetImportJob	授予创建数据集导入作业的权限	Write	datasetImportJob*		
CreateEventTracker	授予创建事件追踪器的权限	Write	eventTracker*		
CreateFilter	授予创建筛选条件的权限	写入	filter*		
CreateMetricAttribution	授予创建指标属性的权限	写入	metricAttribution*		
CreateRecommender	授予创建推荐器的权限	写入	recommender*		
CreateSchema	授予创建架构的权限	Write	schema*		
CreateSolution	授予创建解决方案的权限	Write	solution*		
CreateSolutionVersion	授予创建解决方案版本的权限	Write	solution*		
DeleteCampaign	授予删除活动的权限	Write	campaign*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteDataset	授予删除数据库的权限	Write	dataset*		
DeleteDatasetGroup	授予删除数据集组的权限	Write	datasetGroup*		
DeleteEventTracker	授予删除事件追踪器的权限	Write	eventTracker*		
DeleteFilter	授予删除筛选条件的权限	写入	filter*		
DeleteMetricAttribution	授予删除指标属性的权限	写入	metricAttribution*		
DeleteRecommender	授予删除推荐器的权限	写入	recommender*		
DeleteSchema	授予删除架构的权限。	Write	schema*		
DeleteSolution	授予权限以删除解决方案（包括解决方案的所有版本）	Write	solution*		
DescribeAlgorithm	授予描述算法的权限	Read	algorithm*		
DescribeBatchInferenceJob	授予描述批量推理作业的权限	读取	batchInferenceJob*		
DescribeBatchSegmentJob	授予描述批量分段任务的权限	读取	batchSegmentJob*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeCampaign	授予描述活动的权限	读取	campaign*		
DescribeDataDeletionJob	授予权限以描述数据删除作业	读取	dataDeletionJob*		
DescribeDataInsightsJob	授予权限以描述数据洞察任务	读取	dataInsightsJob*		
DescribeDataset	授予描述数据集的权限	读取	dataset*		
DescribeDatasetExportJob	授予描述数据集导出作业的权限	读取	datasetExportJob*		
DescribeDatasetGroup	授予描述数据集组的权限	Read	datasetGroup*		
DescribeDatasetImportJob	授予描述数据集导入作业的权限	Read	datasetImportJob*		
DescribeEventTracker	授予描述事件追踪器的权限	Read	eventTracker*		
DescribeFeatureTransformation	授予描述功能转换的权限	Read	featureTransformation*		
DescribeFilter	授予描述筛选条件的权限	读取	filter*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeMetricAttribution	授予描述指标属性的权限	读取	metricAttribution*		
DescribeRecipe	授予描述配方的权限	读取	recipe*		
DescribeRecommender	授予权限以描述推荐器	读取	recommender*		
DescribeSchema	授予描述架构的权限	Read	schema*		
DescribeSolution	授予描述解决方案的权限	Read	solution*		
DescribeSolutionVersion	授予描述解决方案版本的权限	读取	solution*		
GetActionRecommendations	授予获取建议操作列表的权限	读取	campaign*		
GetDataInsights	授予权限以从数据洞察任务中获取数据洞察	读取	dataInsightsJob*		
GetPersonalizedRanking	授予权限以获取重新排名的推荐列表	Read	campaign*		
GetRecommendations	授予权限以从活动获取推荐列表	Read	campaign*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetSolutionMetrics	授予权限以为解决方案版本获取指标	Read	solution*		
ListBatchInferenceJobs	授予列出批量推理作业的权限	列表			
ListBatchSegmentJobs	授予权限以列出批量分段任务	列表			
ListCampaigns	授予列出活动的权限	列表			
ListDataDeletionJobs	授予权限以列出数据删除作业	列表			
ListDataInsightsJobs	授予权限以列出数据洞察任务	列表			
ListDatasetExportJobs	授予列出数据集导出作业的权限	列表			
ListDatasetGroups	授予列出数据集组的权限	List			
ListDatasetImportJobs	授予列出数据集导入作业的权限	List			
ListDatasets	授予列出数据集的权限	List			
ListEventTrackers	授予列出事件追踪器的权限	List			
ListFilters	授予列出筛选条件的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListMetricAttributionMetrics	授予列出指标属性指标的权限	列表			
ListMetricAttributions	授予列出指标属性的权限	列表			
ListRecipes	授予列出配方的权限	列表			
ListRecommenders	授予列出推荐器的权限	列表			
ListSchemas	授予列出架构的权限	List			
ListSolutionVersions	授予列出解决方案版本的权限	List			
ListSolutions	授予列出解决方案的权限	列表			
ListTagsForResource	授予权限以列出资源的标签	列表			
PutActionInteractions	授予放置实时操作交互数据的权限	写入			
PutActions	授予摄取操作数据的权限	写入	dataset*		
PutEvents	授予放置实时事件数据的权限	Write			
PutItems	授予提取项目数据的权限	Write	dataset*		
PutUsers	授予提取用户数据的权限	写入	dataset*		
StartRecommender	授予启动推荐器的权限	写入	recommender*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StopRecommender	授予停止推荐器的权限	写入	recommender*		
StopSolutionVersionCreation	授予停止解决方案版本创建的权限	写入	solution*		
TagResource	授予权限以标记资源	Tagging			
UntagResource	授予权限以取消标记资源	标记			
UpdateCampaign	授予更新活动的权限	写入	campaign*		
UpdateDataset	授予更新数据集的权限	写入	dataset*		
UpdateMetricAttribution	授予更新指标属性的权限	写入	metricAttribution*		
UpdateRecommender	授予更新推荐器的权限	写入	recommender*		
UpdateSolution	授予权限以更新解决方案	写入	solution*		

Amazon Personalize 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}	

资源类型	ARN	条件键
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}	

Amazon Personalize 的条件键

Personalize 没有可以在策略语句的 Condition 元素中使用的服务特定上下文键。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon Polly 的操作、资源和条件键

Amazon Polly（服务前缀：polly）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon Polly 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteLexicon	授予删除存储在中的指定发音词典的权限 Amazon Web Services 区域	写入	lexicon*		
DescribeVoices	授予权限以描述在请求语音合成时可用的语音列表	列表			
GetLexicon	授予检索存储在中的指定发音词典内容的权限 Amazon Web Services 区域	读取	lexicon*		
GetSpeechSynthesisTask	授予权限以获取有关特定语音合成任务的信息	读取			
ListLexicons	授予列出存储在中的发音词典的权限 Amazon Web Services 区域	列表			
ListSpeechSynthesisTasks	授予权限以列出请求的语音合成任务	列表			
PutLexicon	授予将发音词典存储在 Amazon Web Services 区域	写入	lexicon*		
StartSpeechSynthesisTask	授予权限以将长输入合成到所提供的 S3 位置	写入	lexicon		s3:PutObject
SynthesizeSpeech	授予权限以合成语音	读取	lexicon		

Amazon Polly 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
lexicon	arn:${Partition}:polly:${Region}:${Account}:lexicon/${LexiconName}	

Amazon Polly 的条件键

Polly 没有可以在策略语句的 Condition 元素中使用的服务特定上下文键。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon Price List 的操作、资源和条件键

Amazon 价目表（服务前缀:pricing）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Price List 定义的操作
- Amazon Price List 定义的资源类型
- Amazon Price List 的条件键

Amazon Price List 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeServices	授予检索所有（已分页）服务的服务详细信息（如果未设置 serviceCode）或特定服务的服务详细信息（如果给定了 serviceCode）的权限	读取			
GetAttributeValues	授予检索给定属性的所有（已分页）可能值的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetPriceListFileUrl	授予权限以检索给定参数的价目表文件 URL	读取			
GetProducts	授予检索具有给定搜索条件的所有匹配产品的权限	读取			
ListPriceLists	授予权限以列出给定参数的所有（分页）合格价目表	读取			

Amazon Price List 定义的资源类型

Amazon 价目表不支持在 IAM 政策声明的`Resource`元素中指定资源 ARN。要允许对 Amazon Price List 的访问权限，请在策略中指定 `"Resource": "*"`。

Amazon Price List 的条件键

价目表没有可以在策略语句的 `Condition` 元素中使用的服务特定上下文键。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon Private Certificate Authority 的操作、资源和条件键

Amazon 私有证书颁发机构（服务前缀:`acm-pca`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Private Certificate Authority 定义的操作
- Amazon Private Certificate Authority 定义的资源类型

- Amazon Private Certificate Authority 的条件键

Amazon Private Certificate Authority 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateCertificateAuthority	授予创建 Amazon 私有 CA 及其关联私钥和配置的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateCertificateAuthorityAuditReport	授予为 Amazon 私有 CA 创建审计报告的权限	写入	certificate-authority*		
CreatePermission	授予为 Amazon 私有 CA 创建权限的权限	权限管理	certificate-authority*		
DeleteCertificateAuthority	授予删除 Amazon 私有 CA 及其关联私钥和配置的权限	写入	certificate-authority*		
DeletePermission	授予删除 Amazon 私有 CA 权限的权限	权限管理	certificate-authority*		
DeletePolicy	授予删除 Amazon 私有 CA 策略的权限	权限管理	certificate-authority*		
DescribeCertificateAuthority	授予返回指定 Amazon 私有 CA 中包含的配置和状态字段列表的权限	读取	certificate-authority*		
DescribeCertificateAuthorityAuditReport	授予返回 Amazon 私有 CA 审计报告的状态和信息的权限	读取	certificate-authority*		
GetCertificate	授予对 ARN 指定的证书颁发机构检索 Amazon 私有 CA 证书和证书链的权限	读取	certificate-authority*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetCertificateAuthorityCertificate	授予对 ARN 指定的证书颁发机构检索 Amazon 私有 CA 证书和证书链的权限	读取	certificate-authority*		
GetCertificateAuthorityCsr	授予权限以检索 ARN 指定的证书颁发机构的 Amazon 私有 CA 证书签名请求 (CSR)	读取	certificate-authority*		
GetPolicy	授予在 Amazon 私有 CA 上检索策略的权限	读取	certificate-authority*		
ImportCertificateAuthorityCertificate	授予将 SSL/TLS 证书导入 Amazon 私有 CA 以用作私有 CA 的 CA 证书的权限 Amazon	写入	certificate-authority*		
IssueCertificate	授予颁发 Amazon 私有 CA 证书的权限	写入	certificate-authority*		
				acm-pca:TemplateArn	
ListCertificateAuthorities	授予权限以检索 Amazon 私有 CA 证书颁发机构 ARNs列表以及调用账户中每个 CA 的状态摘要	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListPermissions	授予列出已应用于 Amazon 私有 CA 证书颁发机构的权限的权限	读取	certificate-authority*		
ListTags	授予列出已应用于 Amazon 私有 CA 证书颁发机构的标签的权限	读取	certificate-authority*		
PutPolicy	授予在 Amazon 私有 CA 上发布策略的权限	权限管理	certificate-authority*		
RestoreCertificateAuthority	授予将 Amazon 私有 CA 从已删除状态恢复到删除时的状态的权限	写入	certificate-authority*		
RevokeCertificate	授予撤销 Amazon 私有 CA 颁发的证书的权限	写入	certificate-authority*		
TagCertificateAuthority	授予向 Amazon 私有 CA 添加一个或多个标签的权限	标记	certificate-authority*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagCertificateAuthority	授予从 Amazon 私有 CA 中移除一个或多个标签的权限	标记	certificate-authority*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys	
UpdateCertificateAuthority	授予更新 Amazon 私有 CA 配置的权限	写入	certificate-authority*		

Amazon Private Certificate Authority 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
certificate-authority	arn:${Partition}:acm-pca:${Region}:${Account}:certificate-authority/${CertificateAuthorityId}	aws:ResourceTag/${TagKey}

Amazon Private Certificate Authority 的条件键

Amazon 私有证书颁发机构定义了以下条件密钥，这些密钥可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
acm-pca:TemplateArn	按颁发证书请求中使用的证书模板的 ARN 筛选访问权限	ARN

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString

Amazon 采购订单控制台的操作、资源和条件键

Amazon 采购订单控制台（服务前缀:purchase-orders）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon 采购订单控制台定义的操作
- Amazon 采购订单控制台定义的资源类型
- Amazon 采购订单控制台的条件键

Amazon 采购订单控制台定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须

具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddPurchaseOrder[仅权限]	授予添加新采购订单的权限	写入	purchase-order*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeletePurchaseOrder[仅权限]	授予删除采购订单的权限	写入	purchase-order*		
				aws:ResourceTag/${TagKey}	
GetConsoleActionSe	授予权限以查看是否使用现有或精细的 IAM 操作来控制对账	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
tEnforced[仅权限]	单、成本管理和账户控制台的授权				
GetPurchaseOrder[仅权限]	授予获取采购订单的权限	读取	purchase-order*		
				aws:ResourceTag/${TagKey}	
ListPurchaseOrderInvoices[仅权限]	授予列出采购订单发票的权限	列表	purchase-order*		
				aws:ResourceTag/${TagKey}	
ListPurchaseOrders[仅权限]	授予列出账户所有采购订单的权限	列表			
ListTagsForResource[仅权限]	授予列出采购订单标签的权限	读取	purchase-order		
				aws:ResourceTag/${TagKey}	
ModifyPurchaseOrders[仅权限]	授予修改采购订单和详细信息的权限	写入	purchase-order*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
TagResource[仅权限]	授予使用给定的键值对标记采购订单的权限	标记	purchase-order*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource[仅权限]	授予从采购订单删除标签的权限	标记	purchase-order*		
				aws:TagKeys aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateConsoleActionSetEnforced[仅权限]	授予权限以更改是使用现有还是精细的 IAM 操作来控制对账单、成本管理和账户控制台的授权	写入			
UpdatePurchaseOrder[仅权限]	授予更新现有采购订单的权限	写入	purchase-order*		
				aws:ResourceTag/${TagKey}	
UpdatePurchaseOrderStatus[仅权限]	授予设置采购订单状态的权限	写入	purchase-order*		
				aws:ResourceTag/${TagKey}	
ViewPurchaseOrders[仅权限]	授予查看采购订单和详细信息的权限	读取	purchase-order		
				aws:ResourceTag/${TagKey}	

Amazon 采购订单控制台定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
purchase-order	arn:${Partition}:purchase-orders::${Account}:purchase-order/${ResourceName}	aws:ResourceTag/${TagKey}

Amazon 采购订单控制台的条件键

Amazon 采购订单控制台定义了以下条件密钥，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中标签的键和值筛选访问	字符串
aws:ResourceTag/${TagKey}	按附加到资源的标签键值对集筛选访问权限	字符串
aws:TagKeys	按请求中的标签键筛选访问	ArrayOfString

Amazon 的操作、资源和条件密钥 QuickSight

Amazon QuickSight （服务前缀:quicksight）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- 亚马逊定义的操作 QuickSight
- Amazon 定义的资源类型 QuickSight
- Amazon 的条件密钥 QuickSight

亚马逊定义的操作 QuickSight

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AccountConfigurations[仅权限]	授予允许设置 Amazon 资源默认访问权限的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchCreateTopicReviewedAnswer	授予权限以为主题创建已审核答案	写入	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
BatchDeleteTopicReviewedAnswer	授予权限以删除主题的已审核答案	写入	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CancelIngestion	授予取消数据集上的 SPICE 摄取的权限	写入	ingestion*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAccountCustomization	授予为账户或命名空间创建 QuickSight 账户自定义项的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateAccountSubscription	授予订阅权限 QuickSight	写入		quicksight:Edition quicksight:DirectoryType	
CreateAdmin[仅权限]	授予配置 Amazon QuickSight 管理员、作者和读者的权限	写入	user*		
CreateAnalysis	授予根据模板创建分析的权限	写入	analysis*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBrand	授予创建亚马逊 QuickSight 品牌的权限	写入	brand*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomPermissions	授予创建 QuickSight 自定义权限资源的权限	写入	custompermissions*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDashboard	授予创建 QuickSight 仪表板的权限	写入	dashboard*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSet	授予创建数据集的权限	Write	datasource*		quicksight:PassDataSource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSource	授予创建数据源的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateEmailCustomizationTemplate[仅权限]	授予创建 QuickSight 电子邮件自定义模板的权限	写入	emailCustomizationTemplate*		
CreateFolder	授予创建 QuickSight 文件夹的权限	写入	folder*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFolderMembership	授予向 QuickSight 文件夹添加 QuickSight 仪表板、分析或数据集的权限	写入	folder*		
			analysis		
			dashboard		
			dataset		
CreateGroup	授予创建 QuickSight 群组的权限	写入	group*		
CreateGroupMembership	授予将 QuickSight 用户添加到群 QuickSight 组的权限	写入	group*	quicksight:UserName	
				aws:TagKeys aws:RequestTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateIAMPolicyAssignment	授予使用指定的 IAM 策略 ARN 创建任务的权限，该分配将分配给指定的群组或用户 QuickSight	写入	assignment*		
CreateIngestion	授予对数据集启动 SPICE 提取的权限	写入	ingestion*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNamespace	授予创建 QuickSight 命名空间的权限	写入	namespace*		ds:CreateIdentityPoolDirectory
CreateReader[仅权限]	授予配置 Amazon QuickSight 读者的权限	写入	user*		
CreateRefreshSchedule	授予为数据集创建刷新计划的权限	写入	refreshschedule*		
CreateRoleMembership	授予为角色添加组成员的权限	写入		quicksight:Group identitystore:GroupId	
CreateTemplate	授予创建模板的权限	Write	template*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTemplateAlias	授予创建模板别名的权限	写入	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTheme	授予创建主题的权限	写入	theme*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateThemeAlias	授予为主题版本创建别名的权限	写入	theme*		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateTopic	授予权限以创建主题	写入	dataset*		quicksight:PassDataSet
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTopicRefreshSchedule	授予权限以为主题创建刷新计划	写入	topic*		
CreateUser[仅权限]	授予配置 Amazon QuickSight 作者和读者的权限	写入	user*		
CreateVPCConnection	授予权限以创建 VPC 连接	写入		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
DeleteAccountCustomization	授予删除账户或命名空间的 QuickSight 账户自定义项的权限	写入	customization*		
DeleteAccountSubscription	授予删除 QuickSight 账户的权限	写入	account*		
DeleteAnalysis	授予删除分析的权限	写入	analysis*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteBrand	授予删除亚马逊 QuickSight 品牌的权限	写入	brand*		
DeleteBrandAssignment	授予删除品牌分配的权限	写入			
DeleteCustomPermissions	授予删除 QuickSight 自定义权限资源的权限	写入			
DeleteDashboard	授予删除 QuickSight 仪表板的权限	写入	dashboard*		
DeleteDataSet	授予删除数据库的权限	写入	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDataSetRefreshProperties	授予删除数据集刷新属性的权限	写入	dataset*		
DeleteDataSource	授予删除数据源的权限	写入	datasource*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDefaultQBusinessApplication	授予删除 QuickSight 账户关联 QBusiness 应用程序的权限	写入			
DeleteEmailCustomizationTemplate[仅权限]	授予删除 QuickSight 电子邮件自定义模板的权限	写入	emailCustomizationTemplate*		
DeleteFolder	授予删除 QuickSight 文件夹的权限	写入	folder*		
DeleteFolderMembership	授予从 QuickSight 文件夹中移除 QuickSight 仪表板、分析或数据集的权限	写入	folder*		
			analysis		
			dashboard		
			dataset		
DeleteGroup	授予从中移除用户组的权限 QuickSight	写入	group*		
DeleteGroupMembership	授予从组中删除用户以使其不再是该组的成员的权限	Write	group*	quicksight:UserName	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteIAMPolicyAssignment	授予更新现有任务的权限	写入	assignment*		
DeleteIdentityPropagationConfig	授予删除用于在中传播可信身份的 Amazon 服务的权限 QuickSight	写入			
DeleteNamespace	授予删除 QuickSight 命名空间的权限	写入	namespace*		ds:DeleteDirectory
DeleteRefreshSchedule	授予删除数据集刷新计划的权限	写入	refreshschedule*		
DeleteRoleCustomPermission	授予移除与角色关联的自定义权限的权限	写入			
DeleteRoleMembership	授予从角色中移除组成员的权限	写入		quicksight:Group identitystore:GroupId	
DeleteTemplate	授予删除模板的权限	Write	template*		
DeleteTemplateAlias	授予删除模板别名的权限	Write	template*		
DeleteTheme	授予删除主题的权限	Write	theme*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteThemeAlias	授予删除主题别名的权限	写入	theme*		
DeleteTopic	授予权限以删除主题	写入	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteTopicRefreshSchedule	授予权限以删除主题刷新计划	写入	topic*		
DeleteUser	根据 QuickSight 用户名，授予删除用户的权限	写入	user*		
DeleteUserByPrincipalId	授予删除由委托人 ID 标识的用户的权限	写入	user*		
DeleteUserCustomPermission	授予移除与用户关联的自定义权限的权限	写入	user*		
DeleteVPCConnection	授予权限以删除 VPC 连接	写入	vpcconnection*		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeAccountCustomization	授予描述账户或命名空间的 QuickSight 账户自定义项的权限	读取	customization*		
DescribeAccountSettings	授予描述账户管理账户设置的 QuickSight 权限	读取			
DescribeAccountSubscription	授予描述 QuickSight 账户的权限	读取	account*		
DescribeAnalysis	授予描述分析的权限	Read	analysis*		
DescribeAnalysisPermissions	授予描述分析权限的权限	读取	analysis*		
DescribeAssetBundleExportJob	授予描述资产包导出作业的权限	读取	assetBundleExportJob*		
DescribeAssetBundleImportJob	授予描述资产包导入作业的权限	读取	assetBundleImportJob*		
DescribeBrand	授予描述品牌的权限	读取	brand*		
DescribeBrandAssignment	授予描述品牌分配的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeBrandPublishedVersion	授予描述品牌已发布版本的权限	读取	brand*		
DescribeCustomPermissions	授予描述 QuickSight 账户中自定义权限资源的权限	读取	custompermissions*		
DescribeDashboard	授予描述 QuickSight 仪表板的权限	读取	dashboard*		
DescribeDashboardPermissions	授予描述 QuickSight 控制面板权限的权限	读取	dashboard*		
DescribeDashboardSnapshotJob	授予权限以描述控制面板快照任务	读取	dashboardSnapshotJob*		
DescribeDashboardSnapshotJobResult	授予权限以描述控制面板快照任务的结果	读取	dashboardSnapshotJob*		
DescribeDashboardsQAConfiguration	授予描述仪表板和配置的权限	读取			
DescribeDataSet	授予描述数据集的权限	Read	dataset*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeDataSetPermissions	授予描述数据集资源策略的权限	权限管理	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeDataSetRefreshProperties	授予描述数据集刷新属性的权限	读取	dataset*		
DescribeDataSource	授予权限以描述数据源	Read	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeDataSourcePermissions	授予描述数据源的资源策略的权限	权限管理	datasource*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeDefaultQBusinessApplication	授予描述 QuickSight 账户关联 QBusiness 应用程序 ID 的权限	读取			
DescribeEmailCustomizationTemplate[仅权限]	授予描述 QuickSight 电子邮件自定义模板的权限	读取	emailCustomizationTemplate*		
DescribeFolder	授予描述 QuickSight 文件夹的权限	读取	folder*		
DescribeFolderPermissions	授予描述 QuickSight 文件夹权限的权限	读取	folder*		
DescribeFolderResolvedPermissions	授予描述已解析 QuickSight 文件夹权限的权限	读取	folder*		
DescribeGroup	授予描述 QuickSight 群组的权限	读取	group*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeGroupMembership	授予描述 QuickSight 群组成员的权限	读取	group*	quicksight:UserName	
DescribeIAMPolicyAssignment	授予描述现有任务的权限	Read	assignment*		
DescribeIngestion	授予描述数据集上 SPICE 提取的权限	读取	ingestion*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeIpRestriction	授予描述 QuickSight 账户 IP 限制的权限	读取			
DescribeKeyRegistration	授予描述 QuickSight 密钥注册的权限	读取			
DescribeNamespace	授予描述 QuickSight 命名空间的权限	读取	namespace*		
DescribeQPersonalizationConfiguration	授予权限以描述个性化配置	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeQuickSightQSearchConfiguration	授予描述 QuickSight Q Search 配置的权限	读取			
DescribeRefreshSchedule	授予描述数据集刷新计划的权限	读取	refreshschedule*		
DescribeRoleCustomPermission	授予描述与角色关联的自定义权限的权限	读取			
DescribeTemplate	授予描述模板的权限	Read	template*		
DescribeTemplateAlias	授予描述模板别名的权限	Read	template*		
DescribeTemplatePermissions	授予描述模板权限的权限	Read	template*		
DescribeTheme	授予描述主题的权限	Read	theme*		
DescribeThemeAlias	授予描述主题别名的权限	Read	theme*		
DescribeThemePermissions	授予描述主题权限的权限	读取	theme*		
DescribeTopic	授予权限以描述主题	读取	topic*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeTopicPermissions	授予权限以描述主题资源策略	权限管理	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeTopicRefresh	授予权限以描述主题刷新状态	读取	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeTopicRefreshSchedule	授予权限以描述主题刷新计划	读取	topic*		
DescribeUser	授予在给定 QuickSight 用户名后描述用户的权限	读取	user*		
DescribeVPCConnection	授予权限以描述 VPC 连接	读取	vpcconnection*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
GenerateEmbedUrlForAnonymousUser	为未注册的用户授予生成用于嵌入 QuickSight 仪表板或 Q 主题的 URL 的权限 QuickSight	写入	namespace* dashboard theme topic		
				aws:TagKeys aws:RequestTag/${TagKey} quicksight:AllowedEmbeddingDomains	
GenerateEmbedUrlForRegisteredUser	授予为注册用户生成用于嵌入 QuickSight 仪表板的 URL 的权限 QuickSight	写入	user*		
				quicksight:AllowedEmbeddingDomains	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GenerateEmbedUrlForRegisteredUserWithIdentity	为 QuickSight 使用身份增强型角色会话注册的用户授予生成用于嵌入 QuickSight 体验的 URL 的权限	写入		quicksight:AllowedEmbeddingDomains	
GetAnonymousUserEmbedUrl[仅权限]	为未注册的用户授予获取用于嵌入 QuickSight 仪表板的 URL 的权限 QuickSight	读取			
GetAuthCode[仅权限]	授予获取代表用户的身份验证码的 QuickSight 权限	读取	user*		
GetDashboardEmbedUrl	授予获取用于嵌入 QuickSight 仪表板的 URL 的权限	读取	dashboard*		
GetGroupMapping[仅权限]	授予在企业版中使用亚马逊 QuickSight识别和显示映射到亚马逊角色的微软活动目录（Microsoft Active Directory）目录组的权限 QuickSight	读取			
GetSessionEmbedUrl	授予获取嵌入 QuickSight 控制台体验的 URL 的权限	读取			
ListAnalyses	授予列出账户中所有分析的权限	列表	analysis*		
ListAssetBundleExportJobs	授予列出所有资产包导出作业的权限	列表	assetBundleExportJob*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListAssetBundleImportJobs	授予列出所有资产包导入作业的权限	列表	assetBundleImportJob*		
ListBrands	授予在 Amazon QuickSight 账户中发布所有品牌的权限	列表			
ListCustomPermissions	授予列出 QuickSight 账户中自定义权限资源的权限	列表			
ListCustomerManagedKeys[仅权限]	授予权限以列出所有注册的客户托管密钥	列表			
ListDashboardVersions	授予列出 QuickSight 控制面板所有版本的权限	列表	dashboard*		
ListDashboards	授予列出 QuickSight 账户中所有仪表板的权限	列表	dashboard*		
ListDataSets	授予列出所有数据集的权限	List		aws:RequestTag/${TagKey} aws:TagKeys	
ListDataSources	授予列出所有数据源的权限	列表		aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListFolderMembers	授予权限以列出所有文件夹的成员	读取	folder*		
ListFolders	授予列出 QuickSight 账户中所有文件夹的权限	列表	folder*		
ListFoldersForResource	授予列出 QuickSight 资源所属的所有文件夹的权限	列表	analysis		
			dashboard		
			dataset		
			datasource		
			topic		
ListGroupMemberships	授予列出组中成员用户的权限	列表	group*		
ListGroups	授予列出中所有用户组的权限 QuickSight	列表	group*		
ListIAMPolicyAssignments	授予列出当前 Amazon QuickSight 账户中所有任务的权限	列表	assignment*		
ListIAMPolicyAssignmentsForUser	授予列出分配给用户及其所属组的所有任务的权限	列表	assignment*		
ListIdentityPropagationConfigs	授予列出为可信身份传播启用的 Amazon 服务的权限 QuickSight	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListIngestions	授予列出数据集中所有 SPICE 提取的权限	列表		aws:RequestTag/${TagKey} aws:TagKeys	
ListKMSKeysForUser[仅权限]	授予权限以列出用户的 KMS 密钥	列表			
ListNamespaces	授予列出账户中所有命名空间的权限 QuickSight	列表			
ListRefreshSchedules	授予列出数据集的所有刷新计划的权限	列表			
ListRoleMemberships	授予列出角色的成员的权限	列表			
ListTagsForResource	授予列出 QuickSight 资源标签的权限	读取	analysis		
			brand		
			customization		
			custompermissions		
			dashboard		
			dataset		
			datasource		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			folder		
			template		
			theme		
			topic		
ListTemplateAliases	授予列出模板的所有别名的权限	List	template*		
ListTemplateVersions	授予列出模板所有版本的权限	列表	template*		
ListTemplates	授予列出 QuickSight 账户中所有模板的权限	列表	template*		
ListThemeAliases	授予列出主题的所有别名的权限	List	theme*		
ListThemeVersions	授予列出主题的所有版本的权限	List	theme*		
ListThemes	授予列出账户中所有主题的权限	列表	theme*		
ListTopicRefreshSchedules	授予权限以列出主题的所有刷新计划	列表			
ListTopicReviewedAnswers	授予权限以列出主题的所有已审核答案	列表		aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListTopics	授予权限以列出所有主题	列表		aws:RequestTag/${TagKey} aws:TagKeys	
ListUserGroups	授予列出给定用户所属组的权限	列表	user*		
ListUsers	授予列出属于该账户的所有 QuickSight 用户的权限	列表	user*		
ListVPCConnections	授予权限以列出所有 VPC 连接	列表		aws:RequestTag/${TagKey} aws:TagKeys	
PassDataSet[仅权限]	授予对模板使用数据集的权限	Read	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PassDataSource[仅权限]	授予对数据集使用数据源的权限	读取	datasource*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
PredictQAResults	授予预测 QA 结果的权限	读取	dashboard		
			topic		
PutDataSetRefreshProperties	授予为数据集添加刷新属性的权限	写入	dataset*		
RegisterCustomerManagedKey[仅权限]	授予权限以注册客户托管密钥	写入			
RegisterUser	授予创建用户的权限，该 QuickSight 用户的身份与请求中指定的 IAM 身份/角色相关联	写入	user*	quicksight:IamArn quicksight:SessionName	
RemoveCustomerManagedKey[仅权限]	授予权限以移除客户托管密钥	写入			
RestoreAnalysis	授予恢复已删除分析的权限	写入	analysis*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ScopeDownPolicy[仅权限]	授予管理资源权限范围策略的权限 Amazon	写入			
SearchAnalyses	授予搜索分析子集的权限	列表	analysis*		
SearchDashboards	授予搜索仪表板子集的 QuickSight 权限	列表	dashboard*		
SearchDataSets	授予搜索子集的权限 QuickSight DatSets	列表	dataset*		
SearchDataSources	授予搜索 QuickSight 数据源子集的权限	列表	datasource*		
SearchDirectoryGroups[仅权限]	授予在企业版中使用亚马逊 QuickSight显示你的 Microsoft Active Directory 目录组的权限，这样你就可以选择将哪些群组映射到亚马逊中的角色 QuickSight	列表			
SearchFolders	授予搜索文件夹子集的 QuickSight 权限	读取	folder*		
SearchGroups	授予搜索群组子集的 QuickSight 权限	列表	group*		
SearchTopics	授予搜索主题子集的权限	列表	topic*		
SearchUsers[仅权限]	授予搜索属于此账户的 QuickSight 用户的权限	列表	user*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
SetGroupMapping[仅权限]	授予在企业版中使用亚马逊 QuickSight显示你的 Microsoft Active Directory 目录组的权限，这样你就可以选择将哪些群组映射到亚马逊中的角色 QuickSight	写入			
StartAssetBundleExportJob	授予启动资产包导出作业的权限	写入	assetBundleExportJob*		
StartAssetBundleImportJob	授予启动资产包导入作业的权限	写入	assetBundleImportJob*		
StartDashboardSnapshotJob	授予权限以启动控制面板快照任务	写入	dashboardSnapshotJob*		
StartDashboardSnapshotJobSchedule	授予权限以启动控制面板快照作业计划	写入			
Subscribe[仅权限]	授予订阅 Amazon 的权限 QuickSight，也允许用户将订阅升级到企业版	写入		quicksight:Edition quicksight:DirectoryType	
TagResource	授予向 QuickSight 资源添加标签的权限	标记	analysis		
			brand		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			customization		
			custompermissions		
			dashboard		
			dataset		
			datasource		
			folder		
			ingestion		
			template		
			theme		
			topic		
			vpcconnection		
				aws:TagKeys aws:RequestTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
Unsubscribe[仅权限]	授予取消订阅亚马逊的权限 QuickSight，这将永久删除亚马逊上的所有用户及其资源 QuickSight	写入			
UntagResource	授予从 QuickSight 资源中移除标签的权限	标记	analysis		
			brand		
			customization		
			custompermissions		
			dashboard		
			dataset		
			datasource		
			folder		
			ingestion		
			template		
			theme		
			topic		
			vpcconnection		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys	
UpdateAccountCustomization	授予更新账户或命名空间的 QuickSight 账户自定义项的权限	写入	customization*		
UpdateAccountSettings	授予更新账户管理员账户设置的 QuickSight 权限	写入			
UpdateAnalysis	授予更新分析的权限	Write	analysis*		
UpdateAnalysisPermissions	授予权限，以更新分析的权限	权限管理	analysis*		
UpdateApplicationWithTokenExchangeGrant	授予使用令牌交换授权更新 QuickSight IAM 身份中心应用程序的权限	写入			
UpdateBrand	授予更新品牌的权限	写入	brand*		
UpdateBrandAssignment	授予更新品牌分配的权限	写入			
UpdateBrandPublishedVersion	授予更新品牌已发布版本的权限	写入	brand*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateCustomPermissions	授予更新 QuickSight 自定义权限资源的权限	写入	custompermissions*		
UpdateDashboard	授予更新 QuickSight 仪表板的权限	写入	dashboard*		
UpdateDashboardLinks	授予更新 QuickSight 控制面板链接的权限	写入	dashboard*		
UpdateDashboardPermissions	授予更新 QuickSight 控制面板权限的权限	权限管理	dashboard*		
UpdateDashboardPublishedVersion	授予更新 QuickSight 仪表板已发布版本的权限	写入	dashboard*		
UpdateDashboardsQAConfiguration	授予更新仪表板 qa 配置的权限	写入			
UpdateDataSet	授予更新数据集的权限	Write	dataset*		quicksight:PassDataSource
			datasource		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateDataSetPermissions	授予更新数据集的资源策略的权限	Permissions management	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateDataSource	授予更新数据源的权限	Write	datasource*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateDataSourcePermissions	授予更新数据源的资源策略的权限	权限管理	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateDefaultQBusinessApplication	授予更新 QuickSight 账户关联 QBusiness 应用程序 ID 的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateEmailCustomizationTemplate[仅权限]	授予更新 QuickSight 电子邮件自定义模板的权限	写入	emailCustomizationTemplate*		
UpdateFolder	授予更新 QuickSight 文件夹的权限	写入	folder*		
UpdateFolderPermissions	授予更新 QuickSight 文件夹权限的权限	权限管理	folder*		
UpdateGroup	授予更改组描述的权限	Write	group*		
UpdateIAMPolicyAssignment	授予更新现有任务的权限	写入	assignment*		
UpdateIdentityPropagationConfig	授予在中添加和更新用于可信身份传播的 Amazon 服务的权限 QuickSight	写入			
UpdateIpRestriction	授予更新 QuickSight 账户 IP 限制的权限	写入			
UpdateKeyRegistration	授予更新 QuickSight 密钥注册的权限	写入			
UpdatePublicSharingSettings	授予在账户上启用或禁用公开共享的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateQPersonalizationConfiguration	授予权限以更新个性化配置	写入			
UpdateQuickSightQSearchConfiguration	授予更新 QuickSight Q Search 配置的权限	写入			
UpdateRefreshSchedule	授予更新数据集刷新计划的权限	写入	refreshschedule*		
UpdateResourcePermissions[仅权限]	授予更新资源级权限的权限 QuickSight	写入			
UpdateRoleCustomPermission	授予更新与角色关联的自定义权限的权限	写入			
UpdateSPICECapacityConfiguration	授予更新 QuickSight SPICE 容量配置的权限	写入			
UpdateTemplate	授予更新模板的权限	Write	template*		
UpdateTemplateAlias	授予更新模板别名的权限	Write	template*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateTemplatePermissions	授予权限，以更新模板的权限	Permissions management	template*		
UpdateTheme	授予更新主题的权限	Write	theme*		
UpdateThemeAlias	授予更新主题别名的权限	Write	theme*		
UpdateThemePermissions	授予权限，以更新主题的权限	权限管理	theme*		
UpdateTopic	授予权限以更新主题	写入	topic*		quicksight:PassDataSet
			dataset		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTopicPermissions	授予权限以更新主题的资源策略	权限管理	topic*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTopicRefreshSchedule	授予权限以更新主题刷新计划	写入	topic*		
UpdateUser	授予更新 Amazon QuickSight 用户的权限	写入	user*		
UpdateUserCustomPermission	授予更新与用户关联的自定义权限的权限	写入	user*		
UpdateVPCConnection	授予权限以更新 VPC 连接	写入	vpcconnection*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	

Amazon 定义的资源类型 QuickSight

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
account	arn:${Partition}:quicksight:${Region}:${Account}:account/${ResourceId}	
user	arn:${Partition}:quicksight:${Region}:${Account}:user/${ResourceId}	
group	arn:${Partition}:quicksight:${Region}:${Account}:group/${ResourceId}	
analysis	arn:${Partition}:quicksight:${Region}:${Account}:analysis/${ResourceId}	aws:ResourceTag/${TagKey}
dashboard	arn:${Partition}:quicksight:${Region}:${Account}:dashboard/${ResourceId}	aws:ResourceTag/${TagKey}
template	arn:${Partition}:quicksight:${Region}:${Account}:template/${ResourceId}	aws:ResourceTag/${TagKey}
vpcconnection	arn:${Partition}:quicksight:${Region}:${Account}:vpcConnection/${ResourceId}	aws:ResourceTag/${TagKey}
assetBundleExportJob	arn:${Partition}:quicksight:${Region}:${Account}:asset-bundle-export-job/${ResourceId}	
assetBundleImportJob	arn:${Partition}:quicksight:${Region}:${Account}:asset-bundle-import-job/${ResourceId}	
datasource	arn:${Partition}:quicksight:${Region}:${Account}:datasource/${ResourceId}	aws:ResourceTag/${TagKey}
dataset	arn:${Partition}:quicksight:${Region}:${Account}:dataset/${ResourceId}	aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
ingestion	arn:${Partition}:quicksight:${Region}:${Account}:dataset/${DatasetId}/ingestion/${ResourceId}	aws:ResourceTag/${TagKey}
refreshschedule	arn:${Partition}:quicksight:${Region}:${Account}:dataset/${DatasetId}/refresh-schedule/${ResourceId}	
theme	arn:${Partition}:quicksight:${Region}:${Account}:theme/${ResourceId}	aws:ResourceTag/${TagKey}
assignment	arn:${Partition}:quicksight::${Account}:assignment/${ResourceId}	
customization	arn:${Partition}:quicksight:${Region}:${Account}:customization/${ResourceId}	aws:ResourceTag/${TagKey}
namespace	arn:${Partition}:quicksight:${Region}:${Account}:namespace/${ResourceId}	
folder	arn:${Partition}:quicksight:${Region}:${Account}:folder/${ResourceId}	aws:ResourceTag/${TagKey}
emailCustomizationTemplate	arn:${Partition}:quicksight:${Region}:${Account}:email-customization-template/${ResourceId}	
topic	arn:${Partition}:quicksight:${Region}:${Account}:topic/${ResourceId}	aws:ResourceTag/${TagKey}
dashboardSnapshotJob	arn:${Partition}:quicksight:${Region}:${Account}:dashboard/${DashboardId}/snapshot-job/${ResourceId}	aws:ResourceTag/${TagKey}
brand	arn:${Partition}:quicksight:${Region}:${Account}:brand/${ResourceId}	aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
custompermissions	arn:${Partition}:quicksight:${Region}:${Account}:custompermissions/${ResourceId}	aws:ResourceTag/${TagKey}

Amazon 的条件密钥 QuickSight

Amazon QuickSight 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中的标签键值对筛选访问	字符串
aws:ResourceTag/${TagKey}	按附加到资源的标签键值对筛选操作	字符串
aws:TagKeys	按标签键筛选访问	ArrayOfString
identitystore:GroupId	按 IdentityStore 群组筛选访问权限 ARN	ARN
quicksight:AllowedEmbeddingDomains	按允许的嵌入域筛选访问权限	ArrayOfString
quicksight:DirectoryType	按照用户管理选项筛选访问权限	字符串
quicksight:Edition	按版本筛选访问权限 QuickSight	字符串

条件键	描述	类型
quicksight:Group	按 QuickSight 群组筛选访问权限 ARN	ARN
quicksight:IamArn	按 IAM 用户或角色 ARN 筛选访问	ARN
quicksight:KmsKeyArns	按 KMS 密钥筛选访问权限 ARNs	ArrayOfARN
quicksight:SessionName	按会话名称筛选访问	字符串
quicksight:UserName	按用户名筛选访问	字符串

Amazon RDS IAM Authentication 的操作、资源和条件键

Amazon RDS IAM 身份验证（服务前缀：`rds-db`）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon RDS IAM Authentication 定义的操作
- Amazon RDS IAM Authentication 定义的资源类型
- 用户 Amazon RDS IAM Authentication 的条件键

Amazon RDS IAM Authentication 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
connect	允许 IAM 角色或用户连接到 RDS 数据库	Permissions management	db-user*		

Amazon RDS IAM Authentication 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从

而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
db-user	arn:${Partition}:rds-db:${Region}:${Account}:dbuser:${DbiResourceId}/${DbUserName}	

用户 Amazon RDS IAM Authentication 的条件键

RDS IAM 身份验证没有可在策略语句的 Condition 元素中使用的服务特定上下文键。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

适用于 Amazon Recycle Bin 的操作、资源和条件键

Amazon 回收站（服务前缀:rbin）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Recycle Bin 定义的操作
- Amazon Recycle Bin 定义的资源类型
- 适用于 Amazon Recycle Bin 的条件键

Amazon Recycle Bin 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateRule	授予权限以创建回收站保留规则	写入	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys rbin:Request/ResourceType	
DeleteRule	授予权限以删除回收站保留规则	写入	rule*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
GetRule	授予权限以获取有关回收站保留规则的详细信息	读取	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
ListRules	授予权限以列出区域中的回收站保留规则	读取		rbin:Request/ResourceType	
ListTagsForResource	授予权限以列出与资源关联的标签	读取	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
LockRule	授予权限以锁定现有的回收站保留规则	写入	rule*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
TagResource	授予权限以添加或更新资源的标签	标记	rule*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys rbin:Attribute/ResourceType	
UnlockRule	授予权限以解锁现有的回收站保留规则	写入	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UntagResource	授予权限以删除与资源关联的标签	标记	rule*		
				aws:ResourceTag/${TagKey} aws:TagKeys rbin:Attribute/ResourceType	
UpdateRule	授予权限以更新现有的回收站保留规则	写入	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	

Amazon Recycle Bin 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
rule	arn:${Partition}:rbin:${Region}:${Account}:rule/${ResourceName}	aws:ResourceTag/${TagKey}

适用于 Amazon Recycle Bin 的条件键

Amazon 回收站定义了以下可以在 IAM 策略Condition元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中标签的键和值筛选访问	字符串
aws:ResourceTag/${TagKey}	根据在请求中是否具有标签键值对来筛选访问权限	字符串
aws:TagKeys	按请求中的标签键筛选访问	ArrayOfString
rbin:Attribute/ResourceType	按现有规则的资源类型筛选访问权限	字符串
rbin:Request/ResourceType	按请求中的资源类型筛选访问权限	字符串

Amazon Redshift 的操作、资源和条件键

Amazon Redshift（服务前缀：redshift）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Redshift 定义的操作

- Amazon Redshift 定义的资源类型
- Amazon Redshift 的条件键

Amazon Redshift 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AcceptReservedNodeExchange	授予在不更改配置的情况下将 DC2 预留节点交换为预留节点的权限 DC1	写入			
AddPartner	授予向集群添加合作伙伴集成的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateDataShareConsumer	授予权限以将使用者与数据共享相关联	Write	datashare*		
				redshift:ConsumerArn redshift:AllowWrites	
AuthorizeClusterSecurityGroupIngress	授予权限以向 Amazon Redshift 安全组添加入站（传入）规则	写入	securitygroup*		
			securitygroupingress-ec2securitygroup*		
AuthorizeDataShare	授予权限以授权指定的数据共享使用者使用数据共享	权限管理	datashare*		
				redshift:ConsumerIdentifier redshift:AllowWrites	
AuthorizeEndpointAccess	授予对 redshift 托管的 VPC 端点的相关活动进行授权的权限	权限管理			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AuthorizeInboundIntegration[仅权限]	授予 Amazon Redshift 权限以持续验证目标数据仓库是否能够接收从源 ARN 复制的数据	写入	integration*		
AuthorizeSnapshotAccess	向指定用户授 Amazon Web Services 账户 予恢复快照的权限	权限管理	snapshot*		
BatchDeleteClusterSnapshots	授予权限以批量删除快照（最多 100 个）	Write	snapshot*		
BatchModifyClusterSnapshots	授予权限以修改快照列表设置	Write	snapshot*		
CancelQuery[仅权限]	授予权限以通过 Amazon Redshift 控制台取消查询	Write			
CancelQuerySession[仅权限]	授予权限以在 Amazon Redshift 控制台中查看查询	Write			
CancelResize	授予权限以取消调整大小操作	Write	cluster*		
CopyClusterSnapshot	授予权限以复制集群快照	写入	snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateAuthenticationProfile	授予权限以创建 Amazon Redshift 身份验证配置文件	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateCluster	授予权限以创建集群	Write	cluster*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterParameterGroup	授予权限以创建 Amazon Redshift 参数组	Write	parametergroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterSecurityGroup	授予权限以创建 Amazon Redshift 安全组	Write	securitygroup*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterSnapshot	授予权限以创建指定集群的手动快照	Write	snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterSubnetGroup	授予权限以创建 Amazon Redshift 子网组	Write	subnetgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterUser	授予权限以自动创建指定的 Amazon Redshift 用户（如果不存在）	权限管理	dbuser*		
				redshift:DbUser	
CreateCustomDomainAssociation	授予权限以为集群创建自定义域名	写入	cluster*		acm:DescribeCertificate

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateEndpointAccess	授予创建 redshift 托管 VPC 端点的权限	写入			
CreateEventSubscription	授予权限以创建 Amazon Redshift 事件通知订阅	Write	eventsubscription*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateHsmClientCertificate	授予权限以创建 HSM 客户端证书，集群在连接到 HSM 时使用该证书	Write	hsmclientcertificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateHsmConfiguration	授予权限以创建 HSM 配置，其中包含集群在硬件安全模块 (HSM) 中存储并使用数据库加密密钥所需的信息	Write	hsmconfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateInboundIntegration[仅权限]	授予源主体权限以创建入站集成，以便将数据从源复制到目标数据仓库	写入			
CreateIntegration	授予权限以创建 Amazon Redshift 零 ETL 集成	写入	integration*		kms:CreateGrant kms:DescribeKey
				aws:RequestTag/${TagKey} aws:TagKeys redshift:IntegrationSourceArn redshift:IntegrationTargetArn	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateQev2IdcApplication[仅权限]	授予权限以创建 qev2 idc 应用程序	写入			sso:CreateApplication sso:PutApplicationAccessScope sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateRedshiftIdcApplication	授予创建 redshift idc 应用程序的权限	写入			sso:CreateApplication sso:PutApplicationAccessScope sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant
CreateSavedQuery[仅权限]	授予权限以通过 Amazon Redshift 控制台创建保存的 SQL 查询	Write			
CreateScheduledAction	授予权限以创建 Amazon Redshift 计划操作	写入			
CreateSnapshotCopyGrant	授予创建快照副本的权限，授予和加密目标中复制的快照的权限 Amazon Web Services 区域	权限管理	snapshotcopygrant*		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateSnapshotSchedule	授予权限以创建快照计划	Write	snapshotschedule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTags	授予权限以将一个或多个标签添加到指定的资源中	Tagging	cluster		
			eventsubscription		
			hsmclientcertificate		
			hsmconfiguration		
			integration		
			parametergroup		
			securitygroup		
			securitygroupingress-cidr		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			securitygroupingress-ec2securitygroup		
			snapshot		
			snapshotcopygrant		
			snapshotschedule		
			subnetgroup		
			usagelimit		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUsageLimit	授予创建使用限制的权限	写入	usagelimit*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
DeauthorizeDataShare	授予权限以删除指定数据共享使用者使用数据共享的权限	权限管理	datashare*		
				redshift:ConsumerIdentifier	
DeleteAuthenticationProfile	授予权限以删除 Amazon Redshift 身份验证配置文件	写入			
DeleteCluster	授予权限以删除以前预配置的集群	Write	cluster*		
DeleteClusterParameterGroup	授予权限以删除 Amazon Redshift 参数组	Write	parametergroup*		
DeleteClusterSecurityGroup	授予权限以删除 Amazon Redshift 安全组	Write	securitygroup*		
DeleteClusterSnapshot	授予权限以删除手动快照	Write	snapshot*		
DeleteClusterSubnetGroup	授予权限以删除集群子网组	写入	subnetgroup*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteCustomDomainAssociation	授予权限以为集群删除自定义域名	写入	cluster*		
DeleteEndpointAccess	授予删除 redshift 托管 VPC 端点的权限	写入			
DeleteEventSubscription	授予权限以删除 Amazon Redshift 事件通知订阅	Write	eventsubscription*		
DeleteHsmClientCertificate	授予权限以删除 HSM 客户端证书	Write	hsmclientcertificate*		
DeleteHsmConfiguration	授予权限以删除 Amazon Redshift HSM 配置	写入	hsmconfiguration*		
DeleteIntegration	授予权限以删除 Amazon Redshift 零 ETL 集成	写入	integration*		
				aws:ResourceTag/${TagKey}	
DeletePartner	授予从集群中删除合作伙伴集成的权限	写入			
DeleteQev2IdcApplication[仅权限]	授予权限以删除 qev2 idc 应用程序	写入	qev2idcapplication*		sso:DeleteApplication

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteRedshiftIdcApplication	授予删除 redshift idc 应用程序的权限	写入	redshiftidcapplication*		sso:DeleteApplication
DeleteResourcePolicy	授予删除指定资源的资源策略的权限	权限管理	namespace*		
DeleteSavedQueries[仅权限]	授予权限以通过 Amazon Redshift 控制台删除保存的 SQL 查询	Write			
DeleteScheduledAction	授予权限以删除 Amazon Redshift 计划操作	Write			
DeleteSnapshotCopyGrant	授予权限以删除快照复制授权	Write	snapshotcopygrant*		
DeleteSnapshotSchedule	授予权限以删除快照计划	Write	snapshotschedule*		
DeleteTags	授予权限以从资源中删除一个或多个标签	Tagging	cluster		
			eventsubscription		
			hsmclientcertificate		
			hsmconfiguration		
			integration		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			parametergroup		
			securitygroup		
			securitygroupingress-cidr		
			securitygroupingress-ec2securitygroup		
			snapshot		
			snapshotcopygrant		
			snapshotschedule		
			subnetgroup		
			usagelimit		
				aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteUsageLimit	授予删除使用限制的权限	写入	usagelimit*		
DeregisterNamespace	授予向使用者注销指定命名空间的权限	写入			
DescribeAccountAttributes	授予描述附加到指定属性的权限 Amazon Web Services 账户	读取			
DescribeAuthenticationProfiles	授予权限以描述已创建的 Amazon Redshift 身份验证配置文件	读取			
DescribeClusterDbRevisions	授予权限以描述集群的数据库修订	List			
DescribeClusterParameterGroups	授予权限以描述 Amazon Redshift 参数组，包括您创建的参数组和默认参数组	Read			
DescribeClusterParameters	授予权限以描述 Amazon Redshift 参数组中包含的参数	Read	parametergroup*		
DescribeClusterSecurityGroups	授予权限以描述 Amazon Redshift 安全组	Read			
DescribeClusterSnapshots	授予权限以描述一个或多个包含集群快照元数据的快照对象	Read			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeClusterSubnetGroups	授予权限以描述一个或多个集群子网组对象，其中包含与集群子网组相关的元数据	Read			
DescribeClusterTracks	授予权限以描述可用维护跟踪	List			
DescribeClusterVersions	授予权限以描述可用 Amazon Redshift 集群版本	Read			
DescribeClusters	授予权限以描述预配置的集群属性	列表			
DescribeCustomDomainAssociations	授予权限以为集群描述自定义域名	列表			
DescribeDataShares	授予权限以描述集群创建和使用的数据共享	Read			
DescribeDataSharesForConsumer	授予权限以仅描述集群使用的数据共享	Read			
DescribeDataSharesForProducer	授予权限以仅描述集群创建的数据共享	Read			
DescribeDefaultClusterParameters	授予权限以描述参数组系列的参数设置	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeEndpointAccess	授予描述 redshift 托管 VPC 端点的权限	读取			
DescribeEndpointAuthorization	授予对 redshift 托管 VPC 端点的描述活动进行授权的权限	列表			
DescribeEventCategories	授予权限以描述所有事件源类型或指定源类型的事件类别	读取			
DescribeEventSubscriptions	授予描述指定的 Amazon Redshift 事件通知订阅的权限 Amazon Web Services 账户	读取			
DescribeEvents	授予权限以描述过去 14 天内与集群、安全组、快照和参数组相关的事件	List			
DescribeHsmClientCertificates	授予权限以描述 HSM 客户端证书	Read			
DescribeHsmConfigurations	授予权限以描述 Amazon Redshift HSM 配置	读取			
DescribeInboundIntegrations	授予列出入站集成的权限	列表		redshift:InboundIntegrationArn	
DescribeIntegrations	授予权限以描述 Amazon Redshift 零 ETL 集成	列表	integration*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey}	
DescribeLoggingStatus	授予权限以描述是否为集群记录信息（例如查询和连接尝试）	Read	cluster*		
DescribeNodeConfigurationOptions	授予权限以描述可能节点配置的属性，例如节点类型、节点数以及指定操作类型的磁盘使用情况。	List			
DescribeOrderableClusterOptions	授予权限以描述可排序集群选项	读取			
DescribePartners	授予检索为集群定义的合作伙伴集成相关信息的权限	读取			
DescribeQev2IdcApplications[仅权限]	授予权限以描述 qev2 idc 应用程序	列表			
DescribeQuery[仅权限]	授予权限以通过 Amazon Redshift 控制台描述查询	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeRedshiftIdcApplications	授予描述 redshift idc 应用程序的权限	列表			sso:GetApplicationGrant sso:ListApplicationAccessScopes
DescribeReservedNodeExchangeStatus	授予权限以描述预留节点交换的交换状态详细信息和关联元数据。状态包括正在进行和请求中的值	读取			
DescribeReservedNodeOfferings	授予权限以描述 Amazon Redshift 提供的可用预留节点产品	Read			
DescribeReservedNodes	授予权限以描述预留节点	Read			
DescribeResize	授予权限以描述集群的上次调整大小操作	Read	cluster*		
DescribeSavedQueries[仅权限]	授予权限以通过 Amazon Redshift 控制台描述已保存查询	Read			
DescribeScheduledActions	授予权限以描述已创建的 Amazon Redshift 计划操作	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeSnapshotCopyGrants	授予描述快照副本的权限授予目标 Amazon Web Services 账户 中指定用户拥有的权限 Amazon Web Services 区域	读取			
DescribeSnapshotSchedules	授予权限以描述快照计划	Read	snapshotschedule*		
DescribeStorage	授予权限以描述账户级备份存储大小和临时存储	Read			
DescribeTable[仅权限]	授予权限以通过 Amazon Redshift 控制台描述表	读取			
DescribeTableRestoreStatus	授予描述使用 RestoreTableFromClusterSnapshot API 操作发出的一个或多个表还原请求状态的权限	读取			
DescribeTags	授予权限以描述标签	Read	cluster		
			eventsubscription		
			hsmclientcertificate		
			hsmconfiguration		
			integration		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			parametergroup		
			securitygroup		
			securitygroupingress-cidr		
			securitygroupingress-ec2securitygroup		
			snapshot		
			snapshotcopygrant		
			snapshotschedule		
			subnetgroup		
			usagelimit		
DescribeUsageLimits	授予描述使用限制的权限	Read	usagelimit*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DisableLogging	授予权限以禁用集群的日志记录信息（例如查询和连接尝试）	Write	cluster*		
DisableSnapshotCopy	授予权限以禁用集群的快照自动复制	Write	cluster*		
DisassociateDataShareConsumer	授予权限以取消使用者与数据共享的关联	Write	datashare*		
				redshift:ConsumerArn	
EnableLogging	授予权限以启用集群的日志记录信息（例如查询和连接尝试）	Write	cluster*		
EnableSnapshotCopy	授予权限以启用集群的快照自动复制	Write	cluster*		
ExecuteQuery[仅权限]	授予权限以通过 Amazon Redshift 控制台执行查询	写入			
FailoverPrimaryCompute	授予从多可用区集群的主计算资源失效转移到另一个可用区的权限	写入	cluster*		
FetchResults[仅权限]	授予权限以通过 Amazon Redshift 控制台提取查询结果	读取			
GetClusterCredentials	授予通过指定用户获取访问亚马逊 Redshift 数据库的临时凭证的权限 Amazon Web Services 账户	写入	dbuser*		
			dbgroup		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			dbname		
				redshift:DbName redshift:DbUser redshift:DurationSeconds	
GetClusterCredentialsWithIAM	授予获取增强型临时凭证的权限，以便通过指定用户访问亚马逊 Redshift 数据库 Amazon Web Services 账户	写入	dbname		
				redshift:DbName redshift:DurationSeconds	
GetReservedNodeExchangeConfigurationOptions	授予权限以获取预留节点交换的配置选项	读取			
GetReservedNodeExchangeOfferings	授予获取与给定 DC1 预留节点 DC2 ReservedNodeOfferings 的付款类型、期限和使用价格相匹配的数组的权限	读取			
GetResourcePolicy	授予获取指定资源的资源策略的权限	读取	namespace*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
JoinGroup	授予权限以加入指定的 Amazon Redshift 组	Permissions management	dbgroup*		
ListDatabases[仅权限]	授予权限以通过 Amazon Redshift 控制台列出数据库	列表			
ListRecommendations	授予权限以列出 Advisor 建议	列表			
ListSavedQueries[仅权限]	授予权限以通过 Amazon Redshift 控制台列出保存的查询	List			
ListSchemas[仅权限]	授予权限以通过 Amazon Redshift 控制台列出架构	List			
ListTables[仅权限]	授予权限以通过 Amazon Redshift 控制台列出表	List			
ModifyAquaConfiguration	授予权限以修改集群的 AQUA 配置	写入	cluster*		
ModifyAuthenticationProfile	授予权限以修改 Amazon Redshift 身份验证配置文件	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ModifyCluster	授予权限以修改集群的设置	Write	cluster*		acm:DescribeCertificate kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:Get

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
					RandomPassword secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
ModifyClusterDbRevision	授予权限以修改集群的数据库修订	写入	cluster*		
ModifyClusterIamRoles	授予修改集群可用来访问其他服务的 Amazon 身份和访问管理 (IAM) Access Management 角色列表的权限 Amazon	权限管理	cluster*		
ModifyClusterMaintenance	授予权限以修改集群的维护设置	Write			
ModifyClusterParameterGroup	授予权限以修改参数组的参数	Write	parametergroup*		
ModifyClusterSnapshot	授予权限以修改快照的设置	Write	snapshot*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ModifyClusterSnapshotSchedule	授予权限以修改集群的快照计划	Write	cluster*		
ModifyClusterSubnetGroup	授予权限以修改集群子网组来包含指定的 VPC 子网列表	写入	subnetgroup*		
ModifyCustomDomainAssociation	授予权限以为集群修改自定义域名	写入	cluster*		acm:DescribeCertificate
ModifyEndpointAccess	授予修改 redshift 托管 VPC 端点的权限	写入			
ModifyEventSubscription	授予权限以修改现有 Amazon Redshift 事件通知订阅	写入	eventsubscription*		
ModifyIntegration	授予权限以修改 Amazon Redshift 零 ETL 集成	写入	integration*		
				aws:ResourceTag/${TagKey}	
ModifyQev2IdcApplication[仅权限]	授予权限以修改 qev2 idc 应用程序	写入	qev2idcapplication*		sso:UpdateApplication

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ModifyRedshiftIdcApplication	授予修改 redshift idc 应用程序的权限	写入	redshiftidcapplication*		sso:DeleteApplicationAccessScope sso:DeleteApplicationGrant sso:GetApplicationGrant sso:ListApplicationAccessScopes sso:PutApplicationAccessScope sso:PutApplicationGrant sso:UpdateApplication
ModifySavedQuery[仅权限]	授予权限以通过 Amazon Redshift 控制台修改现有保存的查询	Write			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ModifyScheduledAction	授予权限以修改现有 Amazon Redshift 计划操作	写入			
ModifySnapshotCopyRetentionPeriod	授予修改从源复制快照 Amazon Web Services 区域后在目标中保留的天数的权限 Amazon Web Services 区域	写入	cluster*		
ModifySnapshotSchedule	授予权限以修改快照计划	Write	snapshotschedule*		
ModifyUsageLimit	授予修改使用限制的权限	Write	usagelimit*		
PauseCluster	授予暂停集群的权限	Write	cluster*		
PurchaseReservedNodeOffering	授予权限以购买预留节点	写入			
PutResourcePolicy	授予更新指定资源的资源策略的权限	权限管理	namespace*		
RebootCluster	授予权限以重新引导集群	写入	cluster*		
RegisterNamespace	向使用者授予注册指定命名空间的权限	写入			
RejectDataShare	授予权限以拒绝另一个账户共享的数据共享	Permissions management	datashare*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ResetClusterParameterGroup	授予权限以将某个参数组的一个或多个参数设为其默认值，并将参数的源值设为“engine-default”	Write	parametergroup*		
ResizeCluster	授予权限以更改集群大小	Write	cluster*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
RestoreFromClusterSnapshot	授予权限以从快照创建集群	Write	cluster*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
			snapshot*		
				aws:TagKeys	
RestoreTableFromClusterSnapshot	授予权限以从 Amazon Redshift 集群快照中的表创建表	Write	cluster*		
			snapshot*		
ResumeCluster	授予权限以恢复集群	写入	cluster*		
RevokeClusterSecurityGroupIngress	授予撤销 Amazon Redshift 安全组中针对先前授权的 IP 范围或亚马逊安全组的入口规则的权限 EC2	写入	securitygroup*		
			securitygroupingress-ec2securitygroup*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
RevokeEndpointAccess	授予对 redshift 托管 VPC 端点中的端点相关活动撤销访问的权限	权限管理			
RevokeSnapshotAccess	授予撤消指定访问权限 Amazon Web Services 账户 以恢复快照的权限	权限管理	snapshot*		
RotateEncryptionKey	授予权限以轮换集群的加密密钥	写入	cluster*		
UpdatePartnerStatus	授予更新合作伙伴集成状态的权限	写入			
ViewQueriesFromConsole[仅权限]	授予权限以通过 Amazon Redshift 控制台查看查询结果	List			
ViewQueriesInConsole[仅权限]	授予权限以通过 Amazon Redshift 控制台终止正在运行的查询和负载	List			

Amazon Redshift 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
cluster	`arn:${Partition}:redshift:${Region}:${Account}:cluster:${ClusterName}`	aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
datashare	arn:${Partition}:redshift:${Region}:${Account}:datashare:${ProducerClusterNamespace}/${DataShareName}	aws:ResourceTag/${TagKey}
dbgroup	arn:${Partition}:redshift:${Region}:${Account}:dbgroup:${ClusterName}/${DbGroup}	
dbname	arn:${Partition}:redshift:${Region}:${Account}:dbname:${ClusterName}/${DbName}	
dbuser	arn:${Partition}:redshift:${Region}:${Account}:dbuser:${ClusterName}/${DbUser}	
eventsubscription	arn:${Partition}:redshift:${Region}:${Account}:eventsubscription:${EventSubscriptionName}	aws:ResourceTag/${TagKey}
hsmclientcertificate	arn:${Partition}:redshift:${Region}:${Account}:hsmclientcertificate:${HSMClientCertificateId}	aws:ResourceTag/${TagKey}
hsmconfiguration	arn:${Partition}:redshift:${Region}:${Account}:hsmconfiguration:${HSMConfigurationId}	aws:ResourceTag/${TagKey}
integration	arn:${Partition}:redshift:${Region}:${Account}:integration:${IntegrationIdentifier}	aws:ResourceTag/${TagKey}
namespace	arn:${Partition}:redshift:${Region}:${Account}:namespace:${ClusterNamespace}	aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
parameter group	arn:${Partition}:redshift:${Region}:${Account}:parametergroup:${ParameterGroupName}	aws:ResourceTag/${TagKey}
securitygroup	arn:${Partition}:redshift:${Region}:${Account}:securitygroup:${SecurityGroupName}/ec2securitygroup/${Owner}/${Ec2SecurityGroupId}	aws:ResourceTag/${TagKey}
securitygroupingress-cidr	arn:${Partition}:redshift:${Region}:${Account}:securitygroupingress:${SecurityGroupName}/cidrip/${IpRange}	aws:ResourceTag/${TagKey}
securitygroupingress-ec2securitygroup	arn:${Partition}:redshift:${Region}:${Account}:securitygroupingress:${SecurityGroupName}/ec2securitygroup/${Owner}/${Ece2SecuritygroupId}	aws:ResourceTag/${TagKey}
snapshot	arn:${Partition}:redshift:${Region}:${Account}:snapshot:${ClusterName}/${SnapshotName}	aws:ResourceTag/${TagKey}
snapshotcopygrant	arn:${Partition}:redshift:${Region}:${Account}:snapshotcopygrant:${SnapshotCopyGrantName}	aws:ResourceTag/${TagKey}
snapshotschedule	arn:${Partition}:redshift:${Region}:${Account}:snapshotschedule:${ScheduleIdentifier}	aws:ResourceTag/${TagKey}
subnetgroup	arn:${Partition}:redshift:${Region}:${Account}:subnetgroup:${SubnetGroupName}	aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
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}	

Amazon Redshift 的条件键

Amazon Redshift 定义了以下可以在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据每个标签的允许值集按操作筛选访问权限	字符串
aws:ResourceTag/${TagKey}	根据与资源关联的标签值，按操作筛选访问权限	字符串
aws:TagKeys	根据在请求中是否具有必需标签按操作筛选访问权限	ArrayOfString
redshift:AllowWrites	按 allowWrites 输入参数筛选访问权限	布尔型
redshift:ConsumerArn	按数据共享使用者 ARN 筛选访问权限	ARN

条件键	描述	类型
redshift:ConsumerIdentifier	按数据共享使用者筛选访问	字符串
redshift:DbName	按数据库名称筛选访问权限	字符串
redshift:DbUser	按数据库用户名筛选访问权限	字符串
redshift:DurationSeconds	根据距临时凭证集到期剩余的秒数筛选访问权限。	字符串
redshift:InboundIntegrationArn	按入站零 ETL 集成资源的 ARN 筛选访问权限	ARN
redshift:IntegrationSourceArn	按零 ETL 集成资源的 ARN 筛选访问权限	ARN
redshift:IntegrationTargetArn	按零 ETL 集成目标的 ARN 筛选访问权限	ARN

Amazon Redshift Data API 的操作、资源和条件键

Amazon Redshift Data API（服务前缀：`redshift-data`）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Redshift Data API 定义的操作

- Amazon Redshift Data API 定义的资源类型
- Amazon Redshift Data API 的条件键

Amazon Redshift Data API 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchExecuteStatement	授予在单个连接下执行多个查询的权限	写入	cluster		
			workgroup		
				redshift-data:sess	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				ion-owner-iam-user id redshift-data:glue-catalog-arn	
CancelStatement	授予权限以取消正在运行的查询	Write		redshift-data:statement-owner-iam-user id	
DescribeStatement	授予权限以检索有关语句执行的详细信息	Read		redshift-data:statement-owner-iam-user id	
DescribeTable	授予权限以检索有关特定表的元数据	Read	cluster*		
			workgroup*		
ExecuteStatement	授予权限以执行查询	写入	cluster		
			workgroup		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				redshift-data:session-owner-iam-userid redshift-data:glue-catalog-arn	
GetStagingBucketLocation	授予获取给定托管工作组的暂存存储桶位置的权限	读取	managed-workgroup*		
GetStatementResult	授予权限以提取查询结果	Read		redshift-data:statement-owner-iam-userid	
ListDatabases	授予权限以列出给定集群的数据库	Read	cluster*		
			workgroup*		
ListSchemas	授予权限以列出给定集群的架构	Read	cluster*		
			workgroup*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListStatements	授予权限以列出给定委托人的查询	List		redshift-data:statement-owner-iam-userid	
ListTables	授予权限以列出给定集群的表	List	cluster*		
			workgroup*		

Amazon Redshift Data API 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
cluster	arn:${Partition}:redshift:${Region}:${Account}:cluster:${ClusterName}	aws:ResourceTag/${TagKey}
workgroup	arn:${Partition}:redshift-serverless:${Region}:${Account}:workgroup/${WorkgroupId}	aws:ResourceTag/${TagKey}
managed-workgroup	arn:${Partition}:redshift-serverless:${Region}:${Account}:managed-workgroup/${ManagedWorkgroupId}	

Amazon Redshift Data API 的条件键

Amazon Redshift Data API 定义以下可以在 IAM policy 的 `Condition` 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:ResourceTag/${TagKey}	按与资源关联的标签值筛选访问权限	字符串
redshift-data:glue-catalog-arn	按胶水目录筛选访问权限 arn	ARN
redshift-data:session-owner-iam-userid	按会话拥有者 IAM 用户 ID 筛选访问权限	字符串
redshift-data:statement-owner-iam-userid	按语句拥有者 IAM 用户 ID 筛选访问权限	字符串

Amazon Redshift Serverless 的操作、资源和条件键

Amazon Redshift Serverless（服务前缀：`redshift-serverless`）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon Redshift Serverless 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ConvertRecoveryPoi	授予将恢复点转换为快照的权限	写入	recoveryPoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ntToSnapshot			snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomDomainAssociation	授予在 Amazon Redshift Serverless 中创建自定义域关联的权限	写入	workgroup*		acm:DescribeCertificate
CreateEndpointAccess	授予创建 Amazon Redshift Serverless 托管 VPC 端点的权限	写入	endpointAccess*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateNamespace	授予创建 Amazon Redshift Serverless 命名空间的权限	写入	namespace*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateScheduledAction	授予为指定的 Amazon Redshift Serverless 命名空间创建计划操作的权限	写入	namespace*		
CreateSnapshot	授予创建命名空间中所有数据库快照的权限	写入	snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshotCopyConfiguration	授予为指定的 Amazon Redshift Serverless 命名空间创建快照复制配置的权限	写入	namespace*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateUsageLimit	授予为指定的 Amazon Redshift Serverless 使用类型创建使用限制的权限	写入			
CreateWorkgroup	授予在 Amazon Redshift Serverless 中创建工作组的权限	写入	workgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCustomDomainAssociation	授予删除自定义域关联的权限	写入	workgroup*		
DeleteEndpointAccess	授予删除 Amazon Redshift Serverless 托管 VPC 端点的权限	写入	endpointAccess*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteNamespace	授予从 Amazon Redshift Serverless 删除命名空间的权限	写入	namespace*		kms:DescribeKey kms:RetireGrant secretsmanager:DeleteSecret secretsmanager:DescribeSecret
DeleteResourcePolicy	授予删除指定资源策略的权限	写入			
DeleteScheduledAction	授予从 Amazon Redshift Serverless 删除计划操作的权限	写入			
DeleteSnapshot	授予从 Amazon Redshift Serverless 删除快照的权限	写入	snapshot*		
DeleteSnapshotCopyConfiguration	授予删除 Amazon Redshift Serverless 命名空间的快照复制配置的权限	写入			
DeleteUsageLimit	授予从 Amazon Redshift Serverless 删除使用限制的权限	写入			
DeleteWorkgroup	授予删除工作组的权限	写入	workgroup*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeOneTimeCredit[仅权限]	授予权限以在 Amazon Redshift Serverless 控制台上查看剩余的免费试用服务抵扣金数量及其到期日期	读取			
GetCredentials	授予获取数据库用户名和临时密码的权限，并获得登录 Amazon Redshift Serverless 的临时授权	写入	workgroup*		
GetCustomDomainAssociation	授予获取特定自定义域关联相关信息的权限	读取	workgroup*		
GetEndpointAccess	授予创建 Amazon Redshift Serverless 托管 VPC 端点的权限	读取	endpointAccess*		
GetManagedWorkgroup	授予使用指定配置设置创建 Amazon Redshift 托管无服务器工作组的权限	读取	managed-workgroup*		
GetNamespace	授予获取有关 Amazon Redshift Serverless 中命名空间信息的权限	读取	namespace*		
GetRecoveryPoint	授予获取有关恢复点的信息的权限	读取	recoveryPoint*		
GetResourcePolicy	授予获取资源策略的权限	读取			
GetScheduledAction	授予获取特定计划操作信息的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetSnapshot	授予获取有关特定快照的信息的权限	读取	snapshot*		
GetTableRestoreStatus	授予获取特定快照的表还原状态的权限	读取			
GetTrack	授予在 Amazon Redshift Serverless 中获取曲目相关信息的权限	读取			
GetUsageLimit	授予获取有关 Amazon Redshift Serverless 中使用限制的信息的权限	读取			
GetWorkgroup	授予获取有关特定工作组的信息的权限	读取	workgroup*		
ListCustomDomainAssociations	授予列出 Amazon Redshift Serverless 中的自定义域关联的权限	列表			
ListEndpointAccess	授予列出 EndpointAccess 对象和相关信息的权限	列表	endpointAccess*		
ListManagedWorkgroups	授予在 Amazon Redshift Serverless 中列出托管工作组的权限	列表			
ListNamespaces	授予列出 Amazon Redshift Serverless 中命名空间的权限	列表			
ListRecoveryPoints	授予列出恢复点数组的权限	列表	namespace		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListScheduledActions	授予列出计划操作的权限	列表			
ListSnapshotCopyConfigurations	授予列出 SnapshotCopyConfiguration 对象和相关信息的权限	列表	namespace		
ListSnapshots	授予列出快照的权限	列表	snapshot*		
ListTableRestoreStatus	授予列出表还原状态的权限	列表			
ListTagsForResource	授予列出分配给资源的标签的权限	列表	namespace		
			workgroup		
				aws:ResourceTag/${TagKey}	
ListTracks	授予列出 Amazon Redshift Serverless 中可用曲目的权限	列表			
ListUsageLimits	授予列出 Amazon Redshift Serverless 中所有使用限制的权限	列表			
ListWorkgroups	授予列出 Amazon Redshift Serverless 中的工作组的权限	列表			
PutResourcePolicy	授予权限以创建或更新资源策略	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
RestoreFromRecoveryPoint	授予从恢复点还原数据的权限	写入	recoveryPoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
RestoreFromSnapshot	授予从快照还原命名空间的权限	写入	snapshot*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
RestoreTableFromRecoveryPoint	授予从恢复点还原表的权限	写入	namespace*		
			recoveryPoint*		
RestoreTableFromSnapshot	授予从快照还原表的权限	写入	namespace*		
			snapshot*		
TagResource	授予将一个或多个标签分配给资源的权限	标记	namespace		
			recoveryPoint		
			snapshot		
			workgroup		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	授予从资源中删除一个或一组标签的权限	标记	namespace		
			recoveryPoint		
			snapshot		
			workgroup		
				aws:TagKeys	
UpdateCustomDomainAssociation	授予更新自定义域所关联的证书的权限	写入	workgroup*		acm:DescribeCertificate
UpdateEndpointAccess	授予更新 Amazon Redshift Serverless 托管 VPC 端点的权限	写入	endpointAccess*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateNamespace	授予使用指定配置设置更新命名空间的权限	写入	namespace*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
UpdateScheduledAction	授予更新计划操作的权限	写入			
UpdateSnapshot	授予更新快照的权限	写入	snapshot*		
UpdateSnapshotCopyConfiguration	授予更新 Amazon Redshift Serverless 命名空间的快照复制配置的权限	写入			
UpdateUsageLimit	授予在 Amazon Redshift Serverless 中更新使用限制的权限	写入			
UpdateWorkgroup	授予使用指定配置设置更新 Amazon Redshift Serverless 工作组的权限	写入	workgroup*		

Amazon Redshift Serverless 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从

而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}	

Amazon Redshift Serverless 的条件键

Amazon Redshift Serverless 定义以下可以在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString
redshift-serverless:endpointAccessId	按端点的访问标识符筛选访问权限	字符串
redshift-serverless:managedWorkgroupName	按托管工作组标识符筛选访问权限	字符串
redshift-serverless:namespaceId	按命名空间标识符筛选访问权限	字符串
redshift-serverless:recoveryPointId	按恢复点标识符筛选访问权限	字符串
redshift-serverless:snapshotId	按快照标识符筛选访问权限	字符串
redshift-serverless:tableRestoreRequestId	按表还原请求标识符筛选访问	字符串

条件键	描述	类型
redshift-serverless:workgroupId	按工作组标识符筛选访问权限	字符串

Amazon Resource Access Manager（RAM）的操作、资源和条件键

Amazon Resource Access Manager (RAMram)（服务前缀:）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Resource Access Manager（RAM）定义的操作
- Amazon Resource Access Manager（RAM）定义的资源类型
- Amazon Resource Access Manager（RAM）的条件键

Amazon Resource Access Manager（RAM）定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AcceptResourceShareInvitation	授予接受指定资源共享邀请的权限	Write	resource-share-invitation*		
				ram:ShareOwnerAccountId ram:ResourceShareName	
AssociateResourceShare	授予将资源和/或委托人与资源共享关联的权限	Write	resource-share*		
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				ram:ResourceShareName ram:AllowsExternalPrincipals ram:Principal ram:RequestedResourceType ram:ResourceArn	
AssociateResourceSharePermission	授予将权限与资源共享关联的权限	写入	customer-managed-permission*		
			permission*		
			resource-share*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreatePermission	授予权限以创建可与资源共享关联的权限	写入		ram:PermissionArn ram:PermissionResourceType aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	ram:TagResource
CreatePermissionVersion	授予权限以创建可与资源共享关联的权限的新版本	写入	customer-managed-permission *		
				ram:PermissionArn ram:PermissionResourceType	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateResourceShare	授予以下权限：使用提供的资源和/或委托人创建资源共享	写入		aws:RequestTag/${TagKey} aws:TagKeys ram:RequestedResourceType ram:ResourceArn ram:RequestedAllowsExternalPrincipals ram:Principal ram:AllowsExternalPrincipals	
DeletePermission	授予权限以删除指定权限	写入	customer-managed-permission *		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} ram:PermissionArn ram:PermissionResourceType	
DeletePermissionVersion	授予权限以删除权限的指定版本	写入	customer-managed-permission*		
				ram:PermissionArn ram:PermissionResourceType	
DeleteResourceShare	授予删除资源共享的权限	Write	resource-share*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals	
DisassociateResourceShare	授予以下权限：取消资源和/或委托人与资源共享的关联	Write	resource-share*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals ram:Principal ram:RequestedResourceType ram:ResourceArn	
DisassociateResourceSharePermission	授予以下权限：取消权限与资源共享的关联	Write	customer-managed-permission*		
			permission*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			resource-share*		
EnableSharingWithAwsOrganization	授予权限以访问客户的组织，并在客户的账户中创建 SLR	权限管理			iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:EnableAWSServiceAccess
GetPermission	授予获取 Amazon RAM 权限内容的权限	读取	customer-managed-permission*		
			permission*		
				ram:PermissionArn	
GetResourcePolicies	授予以下权限：获取您拥有和共享的指定资源的策略	Read			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetResourceShareAssociations	授予以下权限：从提供的列表中获取一组资源共享关联，或者获取具有指定类型的指定状态的资源共享关联	Read			
GetResourceShareInvitations	授予以下权限：按指定邀请 ARN 或资源共享 ARN 获取资源共享邀请	Read			
GetResourceShares	授予以下权限：从提供的列表获取一组资源共享，或获取具有指定状态的资源共享	Read		aws:RequestTag/${TagKey} aws:TagKeys	
ListPendingInvitationResources	授予以下权限：列出资源共享中的特定资源，与您共享这些资源，但邀请仍处于待处理状态	读取	resource-share-invitation*		
				ram:ResourceShareName	
ListPermissionAssociations	授予权限以列出有关权限和任何关联的信息	列表	customer-managed-permission*		
			permission*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				ram:PermissionArn ram:PermissionResourceType	
ListPermissionVersions	授予列出 Amazon RAM 权限版本的权限	列表			
ListPermissions	授予列出 Amazon RAM 权限的权限	列表			
ListPrincipals	授予以下权限：列出您与之共享资源或与您共享了资源的委托人	列表			
ListReplacePermissionAssociationsWork	授予权限以检索异步权限替换的状态	列表			
ListResourceSharePermissions	授予以下权限：列出与资源共享关联的权限	列表	resource-share*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals	
ListResourceTypes	授予列出 Amazon RAM 支持的可共享资源类型的权限	列表			
ListResources	授予以下权限：列出您添加到资源共享的资源或与您共享的资源	列表			
PromotePermissionCreatedFromPolicy	授予权限以创建单独的可完全托管的客户管理型权限	写入	customer-managed-permission*		
				ram:PermissionArn ram:PermissionResourceType	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PromoteResourceShareCreatedFromPolicy	授予提升指定资源共享的权限	Write	resource-share*		
RejectResourceShareInvitation	授予拒绝指定资源共享邀请的权限	写入	resource-share-invitation*		
				ram:ShareOwnerAccountId ram:ResourceShareName	
ReplacePermissionAssociations	授予权限以将所有资源共享更新为新的权限	写入	customer-managed-permission*		
			permission*		
				ram:PermissionArn ram:PermissionResourceType	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
SetDefaultPermissionVersion	授予权限以将某个版本号指定为相应客户管理型权限的默认版本	写入	customer-managed-permission *		
				ram:PermissionArn ram:PermissionResourceType	
TagResource	授予权限以标记指定资源共享或权限	标记	customer-managed-permission		
			resource-share		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予权限以取消标记指定资源共享或权限	标记	customer-managed-permission		
			resource-share		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys	
UpdateResourceShare	授予更新资源共享属性的权限	写入	resource-share*		
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals ram:RequestedAllowsExternalPrincipals	

Amazon Resource Access Manager（RAM）定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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

Amazon Resource Access Manager（RAM）的条件键

Amazon Resource Access Manager (RAM) 定义了以下可用于 IAM 策略Condition元素的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据创建或标记资源共享时在请求中传递的标签筛选访问权限。如果用户不传递这些特定标签，或者根本不指定任何标签，则请求失败	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	根据创建或标记资源共享时传递的标签键筛选访问权限	ArrayOfString
ram:AllowsExternalPrincipals	根据允许或拒绝与外部委托人共享的资源共享筛选访问权限。例如，如果只能对允许与外部委托人共享的资源共享执行该操作，请指定 true。外部委托人是 Amazon 指在其 Amazon 组织之外的账户	布尔型
ram:PermissionArn	根据指定的权限 ARN 筛选访问权限	ARN
ram:PermissionResourceType	根据指定资源类型的权限过滤访问	字符串
ram:Principal	根据指定主体的格式筛选访问权限	字符串
ram:RequestedAllowsExternalPrincipals	按 “allowExternalPrincipals” 的指定值筛选访问权限。外部委托人是 Amazon 指本组织之 Amazon 外的账户	布尔型
ram:RequestedResourceType	根据指定的资源类型筛选访问	字符串
ram:ResourceArn	按指定的 ARN 筛选访问权限	ARN

条件键	描述	类型
ram:ResourceShareName	根据具有指定名称的资源共享筛选访问权限	字符串
ram:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
ram:ShareOwnerAccountId	根据特定账户拥有的资源共享筛选访问权限。例如，您可以使用此条件键指定可以根据资源共享拥有者的账户 ID 接受或拒绝哪些资源共享邀请	字符串

Amazon Resource Group Tagging API 的操作、资源和条件键

Amazon Resource Group Tagging API（服务前缀：`tag`）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Resource Group Tagging API 定义的操作
- Amazon Resource Group Tagging API 定义的资源类型
- Amazon Resource Group Tagging API 的条件键

Amazon Resource Group Tagging API 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeReportCreation	授予描述 StartReportCreation 操作状态的权限	读取			
GetComplianceSummary	授予权限以检索有多少资源不符合其有效标签策略的摘要	读取			
GetResources	授予返回为调用账号指定的已标记或之前标记 Amazon Web Services 区域 的资源的权限	读取			
GetTagKeys	授予返回当前在为调用账户指定的标签密钥 Amazon Web Services 区域 的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetTagValues	授予返回指定密钥的标签值的权限，这些值用于调用账户 Amazon Web Services 区域 的指定密钥	读取			
StartReportCreation	授予权限以开始生成一个报告，其中列出组织中账户的所有已标记资源，以及每个资源是否符合生效标签策略。	写入			
TagResources	授予将一个或多个标签应用到指定资源的权限	标记			
UntagResources	授予从指定资源中删除指定标签的权限	标记			

Amazon Resource Group Tagging API 定义的资源类型

Amazon Resource Group Tagging API 不支持在 IAM policy 语句的 `Resource` 元素中指定资源 ARN。要允许对 Amazon Resource Group Tagging API 的访问权限，请在策略中指定 `"Resource": "*"`。

Amazon Resource Group Tagging API 的条件键

Resource Group Tagging 没有可以在策略语句的 `Condition` 元素中使用的服务特定上下文键。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon Resource Groups 的操作、资源和条件键

Amazon Resource Groups（服务前缀:`resource-groups`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。

- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Resource Groups 定义的操作
- Amazon Resource Groups 定义的资源类型
- Amazon Resource Groups 的条件键

Amazon Resource Groups 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateResource[仅权限]	授予将资源与应用程序关联的权限	写入	group*		
CancelTagSyncTask	授予权限以取消应用程序组标签同步任务	写入	group*		resource-groups:DeleteGroup
CreateGroup	授予创建具有指定名称、描述和资源查询的资源组的权限	Write		aws:RequestTag/${TagKey} aws:TagKeys	cloudformation:DescribeStacks
DeleteGroup	授予删除指定资源组的权限	写入	group*		tag:GetResources
DeleteGroupPolicy[仅权限]	授予权限以为指定组添加基于资源的策略	写入	group*		
DisassociateResource[仅权限]	授予将资源与应用程序取消关联的权限	写入	group*		
GetAccountSettings	授予获取资源组中可选功能的当前状态的权限	读取			
GetGroup	授予获取指定资源组信息的权限	Read	group*		
GetGroupConfiguration	授予获取与指定资源组关联的服务配置的权限	读取	group*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetGroupPolicy[仅权限]	授予权限以获取指定组基于资源的策略	读取	group*		
GetGroupQuery	授予获取与指定资源组关联的查询的权限	读取	group*		
GetTagSyncTask	授予权限以获取指定标签同步任务的信息	读取	group*		
GetTags	授予获取与指定资源组关联的标签的权限	Read	group*		
GroupResources	授予将指定资源添加到指定组的权限	Write	group*		resource-groups:Tag tag:TagResources
ListGroupResources	授予列出属于指定资源组成员的资源的权限	列表	group*		cloudformation:DescribeStacks cloudformation:ListStackResources tag:GetResources
ListGroupingStatuses	授予权限以列出指定应用程序组分组状态	列表	group*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListGroups	授予列出账户中所有资源组的权限	列表			
ListResourceTypes[仅权限]	授予权限以列出支持的资源类型	列表			
ListTagSyncTasks	授予权限以列出账户中的所有标签同步任务	列表	group*		
PutGroupConfiguration	授予放置与指定资源组关联的服务配置的权限	Write	group*		
PutGroupPolicy[仅权限]	授予为指定组添加基于资源的策略的权限	写入	group*		
SearchResources	授予搜索与给定查询匹配的 Amazon 资源的权限	列表			cloudformation:DescribeStacks cloudformation:ListStackResources tag:GetResources
StartTagSyncTask	授予权限以为应用程序组创建标签同步任务	写入	group*		iam:PassRole resource-groups:CreateGroup

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
Tag	授予标记指定资源组的权限	Tagging	group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UngroupResources	授予从指定组中删除指定资源的权限	Write	group*		resource-groups:Untag tag:UntagResources
Untag	授予删除与指定资源组关联的标签的权限	标记	group*		
				aws:TagKeys	
UpdateAccountSettings	授予更新资源组中可选功能的权限	写入			
UpdateGroup	授予更新指定资源组的权限	Write	group*		
UpdateGroupQuery	授予更新与指定资源组关联的查询的权限	Write	group*		cloudformation:DescribeStacks

Amazon Resource Groups 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}

Amazon Resource Groups 的条件键

Amazon Resource Groups 定义了以下可以在 IAM 策略Condition元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对来筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按附加到资源的标签键值对筛选操作	字符串
aws:TagKeys	根据在请求中是否具有标签键来筛选访问	ArrayOfString

Amazon Route 53 的操作、资源和条件键

Amazon Route 53（服务前缀：route53）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon Route 53 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ActivateKeySigningKey	授予激活密钥签名密钥的权限，以使 DNSSEC 可以将其用于签名	Write	hostedzone*		
AssociateVPCWithHostedZone	授予将其他 Amazon VPC 与私有托管区域相关联的权限	写入	hostedzone		ec2:DescribeVpcs
				route53:VPCs	
ChangeCidrCollection	授予在 CIDR 集合中创建或删除 CIDR 块的权限	写入	cidrcollection*		
ChangeResourceRecordSets	授予创建、更新或删除记录的权限，其中包含指定域或子域名称的权威 DNS 信息	Write	hostedzone*		
				route53:ChangeResourceRecordSetsNormalizedRecordNames route53:ChangeResourceRecordSetsRecordTypes route53:ChangeResourceRecor	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				dSetsActions	
ChangeTagsForResource	授予为运行状况检查或托管区域添加、编辑或删除标签的权限	标记	healthcheck*		
			hostedzone*		
CreateCidrCollection	授予创建新的 CIDR 集合的权限	写入			
CreateHealthCheck	授予创建新的运行状况检查的权限，该运行状况检查监控 Web 应用程序、Web 服务器以及其他资源的运行状况和性能	Write			
CreateHostedZone	授予创建公有托管区域的权限，该托管区域用于指定域名系统 (DNS) 如何路由域（如 example.com）及其子域的 Internet 流量	Write		route53:VPCs	ec2:DescribeVpcs
CreateKeySigningKey	授予创建与托管区域关联的新密钥签名密钥的权限	Write	hostedzone*		
CreateQueryLoggingConfig	授予为 DNS 查询日志记录创建配置的权限	Write	hostedzone*		
CreateReusableDelegationSet	授予创建可供多个托管区域重用的委派集（一组四个名称服务器）的权限	Write			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateTrafficPolicy	授予创建流量策略的权限，该流量策略用于为一个域名（如 example.com）或一个子域名（如 www.example.com）创建多个 DNS 记录	Write			
CreateTrafficPolicyInstance	授予基于指定流量策略版本中的设置在指定托管区域中创建记录的权限	Write	hostedzone*		
			trafficpolicy*		
CreateTrafficPolicyVersion	授予创建现有流量策略的新版本的权限	写入	trafficpolicy*		
CreateVPCAssociationAuthorization	授予权限以授权创建指定 VPC 的用户提交关联VPCWithHostedZone 请求，该请求将 VPC 与由其他账户创建的指定托管区域相关联 Amazon Web Services 账户	写入	hostedzone*		
				route53:VPCs	
DeactivateKeySigningKey	授予停用密钥签名密钥的权限，以使 DNSSEC 不会将其用于签名	写入	hostedzone*		
DeleteCidrCollection	授予删除 CIDR 集合的权限	写入	cidrcollection*		
DeleteHealthCheck	授予删除运行状况检查的权限	Write	healthcheck*		
DeleteHostedZone	授予删除托管区域的权限	Write	hostedzone*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteKeySigningKey	授予删除密钥签名密钥的权限	Write	hostedzone*		
DeleteQueryLoggingConfig	授予为 DNS 查询日志记录删除配置的权限	Write	queryloggingconfig*		
DeleteReusableDelegationSet	授予删除可重用委派集的权限	Write	delegationset*		
DeleteTrafficPolicy	授予删除流量策略的权限	Write	trafficpolicy*		
DeleteTrafficPolicyInstance	授予删除流量策略实例以及 Route 53 在您创建该实例时创建的所有记录的权限	Write	trafficpolicyinstance*		
DeleteVPCAssociationAuthorization	授予删除使 Amazon Virtual Private Cloud 与 Route 53 私有托管区域相关联的授权的权限	Write	hostedzone*		
				route53:VPCs	
DisableHostedZoneDNSSEC	授予在特定托管区域中禁用 DNSSEC 签名的权限	Write	hostedzone*		
DisassociateVPCFromHostedZone	授予取消 Amazon Virtual Private Cloud 与 Route 53 私有托管区域的关联的权限	Write	hostedzone		ec2:DescribeVpcs
				route53:VPCs	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
EnableHostedZoneDNSSEC	授予在特定托管区域中启用 DNSSEC 签名的权限	Write	hostedzone*		
GetAccountLimit	授予获取当前账户的指定限制（例如，您使用账户可创建的运行状况检查的最大数量）的权限	Read			
GetChange	授予获取创建、更新或删除一个或多个记录的请求的当前状态的权限	List	change*		
GetCheckerIpRanges	授予获取 Route 53 运行状况检查程序用于检查资源运行状况的 IP 范围列表的权限	List			
GetDNSSEC	授予获取特定托管区域 DNSSEC 信息的权限，包括托管区域中的密钥签名密钥	Read	hostedzone*		
GetGeoLocation	授予获取有关 Route 53 地理位置记录是否支持指定地理位置的信息的权限	List			
GetHealthCheck	授予获取有关指定运行状况检查的信息的权限	读取	healthcheck*		
GetHealthCheckCount	授予获取与当前关联的运行状况检查数量的权限 Amazon Web Services 账户	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetHealthCheckLastFailureReason	授予获取指定运行状况检查最近失败的原因的权限	List	healthcheck*		
GetHealthCheckStatus	授予获取指定运行状况检查的状态的权限	List	healthcheck*		
GetHostedZone	授予获取有关指定托管区域（包括 Route 53 分配给托管区域的四个名称服务器）的信息的权限	列表	hostedzone*		
GetHostedZoneCount	授予获取与当前区域关联的托管区域数量的权限 Amazon Web Services 账户	列表			
GetHostedZoneLimit	授予获取指定托管区域的指定限制的权限	Read	hostedzone*		
GetQueryLoggingConfig	授予获取有关 DNS 查询日志记录的指定配置的信息的权限	Read	queryloggingconfig*		
GetReusableDelegationSet	授予获取有关指定可重用委派集（包括分配给委派集的四个名称服务器）的信息的权限	List	delegationset*		
GetReusableDelegationSetLimit	授予获取可与指定可重用委派集关联的托管区域的最大数量的权限	Read	delegationset*		
GetTrafficPolicy	授予获取有关指定流量策略版本的信息的权限	Read	trafficpolicy*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetTrafficPolicyInstance	授予获取有关指定流量策略实例的信息的权限	读取	trafficpolicyinstance*		
GetTrafficPolicyInstanceCount	授予获取与当前流量策略关联的流量策略实例数量的权限 Amazon Web Services 账户	读取			
ListCidrBlocks	授予获取指定 CIDR 集合中 CIDR 块列表的权限	列表	cidrcollection*		
ListCidrCollections	授予获取与当前 CIDR 集合关联的 CIDR 集合列表的权限 Amazon Web Services 账户	列表			
ListCidrLocations	授予获取属于指定 CIDR 集合的 CIDR 位置列表的权限	列表	cidrcollection*		
ListGeoLocations	授予获取对于地理位置 Route 53 支持的地理位置列表的权限	读取			
ListHealthChecks	授予获取与当前状态关联的运行状况检查列表的权限 Amazon Web Services 账户	读取			
ListHostedZones	授予获取与当前托管区域关联的公共和私有托管区域列表的权限 Amazon Web Services 账户	列表			
ListHostedZonesByName	授予获取按词典顺序排列的您的托管区域列表的权限。托管区域按名称进行排序并颠倒了标签，例如 com.example.www。	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListHostedZonesByVPC	授予权限以获取与指定的 VPC 关联的所有私有托管区域的列表	列表		route53:VPCs	ec2:DescribeVpcs
ListQueryLoggingConfigs	授予列出与当前 Amazon Web Services 账户 或与指定托管区域关联的配置关联的 DNS 查询日志记录配置的权限	列表	hostedzone		
ListResourceRecordSets	授予列出指定托管区域中的记录的权限	列表	hostedzone*		
ListReusableDelegationSets	授予权限以列出与当前 Amazon Web Services 账户关联的可重用委派集。	读取			
ListTagsForResource	授予列出一个运行状况检查或托管区域的标签的权限	读取	healthcheck		
			hostedzone		
ListTagsForResources	授予列出最多 10 个运行状况检查或托管区域的标签的权限	读取	healthcheck		
			hostedzone		
ListTrafficPolicies	授予权限以获取有关与当前 Amazon Web Services 账户关联的每个流量策略的最新版本的信息。策略按创建顺序列出	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListTrafficPolicyInstances	授予权限以获取有关您使用当前流量策略创建的流量策略实例的信息 Amazon Web Services 账户	读取			
ListTrafficPolicyInstancesByHostedZone	授予获取有关您在指定托管区域中创建的流量策略实例的信息的权限	List	hostedzone*		
ListTrafficPolicyInstancesByPolicy	授予获取有关您使用指定流量策略版本创建的流量策略实例的信息的权限	List	trafficpolicy*		
ListTrafficPolicyVersions	授予获取有关指定流量策略的所有版本的信息的权限	列表	trafficpolicy*		
ListVPCAssociationAuthorizations	授予权限以获取由其他账户创建 VPCs 的、可以与指定托管区域关联的列表	列表	hostedzone*		
TestDNSAnswer	授予获取 Route 53 为响应指定记录名称和类型的 DNS 查询而返回的值的权限	Read			
UpdateHealthCheck	授予更新现有运行状况检查的权限	Write	healthcheck*		
UpdateHostedZoneComment	授予更新指定托管区域的注释的权限	Write	hostedzone*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateTrafficPolicyComment	授予更新指定流量策略版本的注释的权限	Write	trafficpolicy*		
UpdateTrafficPolicyInstance	授予更新指定托管区域中基于指定流量策略版本中的设置创建的记录的权限	Write	trafficpolicyinstance*		

Amazon Route 53 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
cidrcollection	arn:${Partition}:route53:::cidrcollection/${Id}	
change	arn:${Partition}:route53:::change/${Id}	
delegationset	arn:${Partition}:route53:::delegationset/${Id}	
healthcheck	arn:${Partition}:route53:::healthcheck/${Id}	
hostedzone	arn:${Partition}:route53:::hostedzone/${Id}	
trafficpolicy	arn:${Partition}:route53:::trafficpolicy/${Id}	

资源类型	ARN	条件键
trafficpolicyinstance	arn:${Partition}:route53:::trafficpolicyinstance/${Id}	
queryloggingconfig	arn:${Partition}:route53:::queryloggingconfig/${Id}	
vpc	arn:${Partition}:ec2:${Region}:${Account}:vpc/${VpcId}	

Amazon Route 53 的条件键

Amazon Route 53 定义以下可在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
route53:ChangeResourceRecordSetsActions	按请求中的更改操作 “创建”、“UPSERT” 或 “删除” 筛选访问权限 ChangeResourceRecordSets	ArrayOfString
route53:ChangeResourceRecordSetsNormalizedRecordNames	按 ChangeResourceRecordSets 请求中的标准化 DNS 记录名称筛选访问权限	ArrayOfString
route53:ChangeResourceRecordSetsRecordTypes	按 ChangeResourceRecordSets 请求中的 DNS 记录类型筛选访问权限	ArrayOfString

条件键	描述	类型
route53:VPCs	按 VPCs 请求筛选访问权限	ArrayOfString

Amazon Route 53 Resolver 的操作、资源和条件键

Amazon Route 53 Resolver（服务前缀：`route53resolver`）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Route 53 Resolver 定义的操作
- Amazon Route 53 Resolver 定义的资源类型
- Amazon Route 53 Resolver 的条件键

Amazon Route 53 Resolver 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateFirewallRuleGroup	授予将 Amazon VPC 与指定的防火墙规则组关联的权限	Write	firewall-rule-group-association*		ec2:DescribeVpcs
				aws:RequestTag/${TagKey} aws:TagKeys	
AssociateResolverEndpointIpAddress	授予权限以将指定的 IP 地址与解析程序终端节点相关联。这是 DNS 查询在通往您的网络（出站）或您的网络 VPCs（入站）的途中通过的 IP 地址	写入	resolver-endpoint*		ec2:CreateNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateResolverQueryLogConfig	授予权限以将 Amazon VPC 与指定查询日志记录配置关联	Write	resolver-query-log-config*		ec2:DescribeVpcs
AssociateResolverRule	授予权限以将指定的解析程序规则与指定的 VPC 相关联	Write	resolver-rule*		ec2:DescribeVpcs
CreateFirewallDomainList	授予创建防火墙域列表的权限	Write	firewall-domain-list*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFirewallRule	授予在防火墙规则组中创建防火墙规则的权限	Write	firewall-domain-list*		
			firewall-rule-group*		
CreateFirewallRuleGroup	授予创建防火墙规则组的权限	写入	firewall-rule-group*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateOutpostResolver	授予权限以在 Outposts 上创建 Route 53 Resolver	写入	outpost-resolver*		outposts:GetOutpost
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateResolverEndpoint	授予权限以创建解析程序终端节点 共有两种类型的解析程序终端节点：入站和出站。	写入	resolver-endpoint*		ec2:CreateNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateResolverQueryLogConfig	授予创建 Resolver 查询日志配置的权限，该配置定义了你希望 Resolver 在哪里保存源自你的 DNS 查询日志 VPCs	写入		aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateResolverRule	授予权限以定义如何将来自您的 VPC 的查询路由到 VPC 之外	写入	resolver-rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFirewallDomainList	授予删除防火墙域列表的权限	Write	firewall-domain-list*		
DeleteFirewallRule	授予删除防火墙规则组中的防火墙规则的权限	Write	firewall-domain-list*		
			firewall-rule-group*		
DeleteFirewallRuleGroup	授予删除防火墙规则组的权限	写入	firewall-rule-group*		
DeleteOutpostResolver	授予权限以在 Outposts 上删除 Route 53 Resolver	写入	outpost-resolver*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteResolverEndpoint	授予权限以删除解析程序终端节点。删除解析程序终端节点的效果取决于它是入站还是出站终端节点	Write	resolver-endpoint*		ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces
DeleteResolverQueryLogConfig	授予权限以删除解析程序查询日志记录配置	Write	resolver-query-log-config*		
DeleteResolverRule	授予权限以删除解析程序规则	Write	resolver-rule*		
DisassociateFirewallRuleGroup	授予删除指定防火墙规则组与指定 VPC 之间的关联的权限	Write	firewall-rule-group-association*		
DisassociateResolverEndpointIpAddress	授予权限以从解析程序终端节点中删除指定的 IP 地址。这是 DNS 查询在通往您的网络（出站）或您的网络 VPCs（入站）的途中通过的 IP 地址	写入	resolver-endpoint*		ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces
DisassociateResolverQueryLogConfig	授予权限以删除指定解析程序查询日志记录配置与指定 VPC 之间的关联	Write	resolver-query-log-config*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DisassociateResolverRule	授予权限以删除指定解析程序规则与指定 VPC 之间的关联	Write	resolver-rule*		
GetFirewallConfig	授予获取有关指定防火墙配置信息的权限	Read	firewall-config*		ec2:DescribeVpcs
GetFirewallDomainList	授予获取有关指定防火墙域列表信息的权限	Read	firewall-domain-list*		
GetFirewallRuleGroup	授予获取有关指定防火墙规则组信息的权限	Read	firewall-rule-group*		
GetFirewallRuleGroupAssociation	授予获取有关指定防火墙规则组与 VPC 之间关联的信息的权限	读取	firewall-rule-group-association*		
GetFirewallRuleGroupPolicy	授予获取有关指定防火墙规则组策略信息的权限，该策略指定了您要允许其他 Amazon Web Services 账户 人使用的防火墙规则组操作和资源	读取	firewall-rule-group*		
GetOutpostResolver	授予权限以获取 Outposts 上指定 Route 53 Resolver 的信息	读取	outpost-resolver*		
GetResolverConfig	授予权限以在指定资源中获取解析程序配置状态	读取	resolver-config*		ec2:DescribeVpcs
GetResolverDnssecConfig	授予获取指定资源内 DNS 查询的 DNSSEC 验证支持状态的权限	Read	resolver-dnssec-config*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetResolverEndpoint	授予权限以获取有关指定解析程序终端节点的信息，例如，它是入站还是出站终端节点，DNS 查询转发到您的 VPC 时经过的 IP 地址以及从您的 VPC 转发时经过的 IP 地址	读取	resolver-endpoint*		
GetResolverQueryLogConfig	授予权限以获取有关指定 Resolver 查询日志配置的信息，例如 VPCs 该配置记录查询的数量和日志发送到的位置	读取	resolver-query-log-config*		ec2:DescribeVpcs
GetResolverQueryLogConfigAssociation	授予权限以获取解析程序查询日志记录配置与 Amazon VPC 之间指定关联的信息 当您将 VPC 与查询日志记录配置相关联时，解析程序会记录源自该 VPC 的 DNS 查询	读取			
GetResolverQueryLogConfigPolicy	授予权限以获取有关指定 Resolver 查询日志记录策略的信息，该策略指定您想要允许其他 Amazon Web Services 账户 人使用的解析器查询日志操作和资源	读取	resolver-query-log-config*		
GetResolverRule	授予权限以获取有关指定解析程序规则的信息，例如，规则为其转发 DNS 查询的域名以及将查询转发到的 IP 地址	Read	resolver-rule*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetResolverRuleAssociation	授予权限以获取有关指定解析程序规则与 VPC 之间的关联的信息	读取	resolver-rule*		
GetResolverRulePolicy	授予获取有关 Resolver 规则策略信息的权限，该策略指定了你想允许其他 Amazon Web Services 账户 人使用的解析器操作和资源	读取	resolver-rule*		
ImportFirewallDomains	授予在防火墙域列表中添加、删除或替换防火墙域的权限	写入	firewall-domain-list*		
ListFirewallConfigs	授予列出当前 Amazon Web Services 账户 可以检查的所有防火墙配置的权限	列表			ec2:DescribeVpcs
ListFirewallDomainLists	授予列出当前 Amazon Web Services 账户 能够使用的所有防火墙域列表的权限	列表			
ListFirewallDomains	授予列出指定防火墙域列表下所有防火墙域的权限	列表	firewall-domain-list*		
ListFirewallRuleGroupAssociations	授予列出有关 Amazon VPCs 和 Firewall 规则组之间关联信息的权限	列表			
ListFirewallRuleGroups	授予列出当前 Amazon Web Services 账户 能够使用的所有防火墙规则组的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListFirewallRules	授予列出指定防火墙规则组下所有防火墙规则的权限	列表	firewall-rule-group*		
ListOutpostResolvers	授予列出 Outposts 上所有使用当前版本创建的 Route 53 Resolver 实例的权限 Amazon Web Services 账户	列表			
ListResolverConfigs	授予权限以列出解析程序配置状态	列表	resolver-config*		ec2:DescribeVpcs
ListResolverDnssecConfigs	授予列出 DNS 查询的 DNSSEC 验证支持状态的权限	列表	resolver-dnssec-config*		
ListResolverEndpointIpAddresses	授予列出 DNS 查询在通往您的网络（出站）或指定 Resolver 终端节点的 VPCs （入站）途中通过的 IP 地址的权限	列表	resolver-endpoint*		
ListResolverEndpoints	授予列出使用当前 Resolver 创建的所有解析器端点的权限 Amazon Web Services 账户	列表			
ListResolverQueryLogConfigAssociations	授予列出有关 Amazon VPCs 和查询日志配置之间关联的信息的权限	列表			ec2:DescribeVpcs

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListResolverQueryLogConfigs	授予列出有关指定查询日志配置的信息的权限，这些配置定义了您希望 Resolver 将 DNS 查询日志保存在何处 VPCs ，并指定要为其记录查询的内容	列表			ec2:DescribeVpcs
ListResolverRuleAssociations	授予列出在 Resolver 规则和 VPCs 使用当前规则之间创建的关联的权限 Amazon Web Services 账户	列表			ec2:DescribeVpcs
ListResolverRules	授予列出使用当前规则创建的解析器规则的权限 Amazon Web Services 账户	列表			
ListTagsForResource	授予权限以列出与指定资源关联的标签	读取	firewall-domain-list		
			firewall-rule-group		
			firewall-rule-group-association		
			outpost-resolver		
			resolver-endpoint		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			resolver-query-log-config		
			resolver-rule		
PutFirewallRuleGroupPolicy	授予权限以指定 Amazon Web Services 账户 要与之共享的防火墙规则组、要共享的防火墙规则组以及您希望该帐户能够对配置执行的操作	权限管理	firewall-rule-group*		
PutResolverQueryLogConfigPolicy	授予权限 Amazon Web Services 账户 以指定要与之共享查询日志配置的、要共享的查询日志配置以及您希望该账户能够对配置执行的操作	权限管理	resolver-query-log-config*		
PutResolverRulePolicy	授予权限以指定 Amazon Web Services 账户 要与之共享的规则、要共享的解析器规则以及您希望该账户能够对这些规则执行的操作	权限管理	resolver-rule*		
TagResource	授予权限以将一个或多个标签添加到指定的资源中	Tagging	firewall-config		
			firewall-domain-list		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			firewall-rule-group		
			firewall-rule-group-association		
			outpost-resolver		
			resolver-dnssec-config		
			resolver-endpoint		
			resolver-query-log-config		
			resolver-rule		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予权限以从指定的资源中删除一个或多个标签	Tagging	firewall-config		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			firewall-domain-list		
			firewall-rule-group		
			firewall-rule-group-association		
			outpost-resolver		
			resolver-dnssec-config		
			resolver-endpoint		
			resolver-query-log-config		
			resolver-rule		
				aws:TagKeys	
UpdateFirewallConfig	授予更新防火墙配置的选定设置的权限	Write	firewall-config*		ec2:DescribeVpcs

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateFirewallDomains	授予在防火墙域列表中添加、删除或替换防火墙域的权限	Write	firewall-domain-list*		
UpdateFirewallRule	授予更新防火墙规则组中防火墙规则的选定设置的权限	Write	firewall-domain-list*		
			firewall-rule-group*		
UpdateFirewallRuleGroupAssociation	授予更新防火墙规则组关联的选定设置的权限	写入	firewall-rule-group-association*		
UpdateOutpostResolver	授予权限以更新 Outposts 上指定 Route 53 Resolver 的选定设置	写入	outpost-resolver*		
UpdateResolverConfig	授予权限以在指定资源中更新解析程序配置状态	写入	resolver-config*		ec2:DescribeVpcs
UpdateResolverDnssecConfig	授予更新指定资源内 DNS 查询的 DNSSEC 验证支持状态的权限	Write	resolver-dnssec-config*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateResolverEndpoint	授予权限以更新为入站或出站解析程序终端节点选择的设置	Write	resolver-endpoint*		ec2:AssignIpv6Addresses ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:ModifyNetworkInterfaceAttribute ec2:UnassignIpv6Addresses
UpdateResolverRule	授予权限以更新指定解析程序规则的设置	Write	resolver-rule*		

Amazon Route 53 Resolver 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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/${TagKey}
resolver-endpoint	arn:${Partition}:route53resolver:${Region}:${Account}:resolver-endpoint/${ResourceId}	aws:ResourceTag/${TagKey}
firewall-rule-group	arn:${Partition}:route53resolver:${Region}:${Account}:firewall-rule-group/${ResourceId}	aws:ResourceTag/${TagKey}
firewall-rule-group-association	arn:${Partition}:route53resolver:${Region}:${Account}:firewall-rule-group-association/${ResourceId}	aws:ResourceTag/${TagKey}
firewall-domain-list	arn:${Partition}:route53resolver:${Region}:${Account}:firewall-domain-list/${ResourceId}	aws:ResourceTag/${TagKey}
firewall-config	arn:${Partition}:route53resolver:${Region}:${Account}:firewall-config/${ResourceId}	aws:ResourceTag/${TagKey}
resolver-config	arn:${Partition}:route53resolver:${Region}:${Account}:resolver-config/${ResourceId}	

资源类型	ARN	条件键
outpost-resolver	arn:${Partition}:route53resolver:${Region}:${Account}:outpost-resolver/${ResourceId}	aws:ResourceTag/${TagKey}

Amazon Route 53 Resolver 的条件键

Amazon Route 53 Resolver 定义以下可在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对来筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按是否存在附加到资源的标签键值对筛选访问权限	字符串
aws:TagKeys	根据在请求中是否具有标签键来筛选访问	ArrayOfString

Amazon S3 Glacier 的操作、资源和条件键

Amazon S3 Glacier（服务前缀：glacier）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon S3 Glacier 定义的操作

- Amazon S3 Glacier 定义的资源类型
- Amazon S3 Glacier 的条件键

Amazon S3 Glacier 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AbortMultipartUpload	授予权限以中止由上传 ID 标识的分段上传操作	写入	vault*		
AbortVaultLock	授予权限以在文件库锁定未处于锁定状态时中止文件库锁定过程	权限管理	vault*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddTagsToVault	授予权限以向文件库添加指定的标签	标记	vault*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CompleteMultipartUpload	授予权限以完成分段上传过程	写入	vault*		
CompleteVaultLock	授予权限以完成文件库锁定过程	权限管理	vault*		
CreateVault	授予权限以使用指定名称建立新的文件库	写入	vault*		
DeleteArchive	授予权限以从文件库中删除档案	写入	vault*		
				glacier:ArchiveAgeInDays	
DeleteVault	授予权限以删除文件库	写入	vault*		
DeleteVaultAccessPolicy	授予权限以删除与指定文件库关联的访问策略	权限管理	vault*		
DeleteVaultNotifications	授予权限以删除为文件库设置的通知配置	写入	vault*		
DescribeJob	授予权限以获取有关以前启动的任务的信息	读取	vault*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeVault	授予权限以获取有关文件库的信息	读取	vault*		
GetDataRetrievalPolicy	授予权限以获取数据检索策略	读取			
GetJobOutput	授予权限以下载指定任务的输出	读取	vault*		
GetVaultAccessPolicy	授予权限以检索在文件库中设置的访问策略子资源	读取	vault*		
GetVaultLock	授予权限以从指定文件库上设置的锁定策略子资源中检索属性	读取	vault*		
GetVaultNotifications	授予权限以检索在文件库中设置的通知配置子资源	读取	vault*		
InitiateJob	授予权限以启动指定类型的任务	写入	vault*		
				glacier:ArchiveAgeInDays	
InitiateMultipartUpload	授予权限以启动分段上传	写入	vault*		
InitiateVaultLock	授予权限以启动文件库锁定过程	权限管理	vault*		
ListJobs	授予权限以列出文件库的任务，包括正在进行的任务以及最近完成的任务	列表	vault*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListMultipartUploads	授予权限以列出指定文件库所有正在进行的分段上传	列表	vault*		
ListParts	授予权限以列出已在特定分段上传中上传的档案部分	列表	vault*		
ListProvisionedCapacity	授予列出指定容量的预配置容量的权限 Amazon Web Services 账户	列表			
ListTagsForVault	授予权限以列出已连接至文件库的所有标签	列表	vault*		
ListVaults	授予权限以列出所有文件库	列表			
PurchaseProvisionedCapacity	授予购买预配置容量单位的权限 Amazon Web Services 账户	写入			
RemoveTagsFromVault	授予权限以从已连接至文件库的标签集中删除一个或多个标签	标记	vault*		
SetDataRetrievalPolicy	授予权限以在 PUT 请求指定的区域中设置数据检索策略，然后应用此策略	权限管理			
SetVaultAccessPolicy	授予权限以为文件库配置访问策略；这将覆盖现有策略	权限管理	vault*		
SetVaultNotifications	授予权限以配置文件库通知	写入	vault*		
UploadArchive	授予权限以将档案上传到文件库	写入	vault*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UploadMultipartPart	授予权限以上传档案的一部分	写入	vault*		

Amazon S3 Glacier 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
vault	arn:${Partition}:glacier:${Region}:${Account}:vaults/${VaultName}	

Amazon S3 Glacier 的条件键

Amazon S3 Glacier 定义以下可在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString
glacier:ArchiveAgeInDays	按照档案已在文件库中存储的时间长度（以天为单位）筛选访问权限。	字符串

条件键	描述	类型
glacier:ResourceTag/	按客户定义的标签筛选访问权限	字符串

Amazon S3 Object Lambda 的操作、资源和条件键

Amazon S3 Object Lambda（服务前缀：`s3-object-lambda`）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon S3 Object Lambda 定义的操作
- Amazon S3 Object Lambda 定义的资源类型
- Amazon S3 Object Lambda 的条件键

Amazon S3 Object Lambda 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AbortMultipartUpload	授予权限以中止分段上传	Write	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
DeleteObject	授予权限以删除对象的空版本并插入删除标记，此版本成为对象的当前版本	写入	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
DeleteObjectTagging	授予权限以使用标记子资源从指定的对象中删除整个标记集	标记	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
DeleteObjectVersion	授予权限以删除特定版本的对象	写入	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
DeleteObjectVersionTagging	授予权限以删除特定版本对象的整个标记集	Tagging	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
GetObject	授予权限以从 Amazon S3 检索对象	读取	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectAcl	授予权限以返回对象的访问控制列表 (ACL)	Read	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectLegalHold	授予权限以获取对象的当前依法保留状态	读取	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectRetention	授予权限以检索对象的保留设置	读取	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectTagging	授予权限以返回对象的标签集	Read	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectVersion	授予权限以检索对象的特定版本	读取	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
GetObjectVersionAcl	授予权限以返回特定对象版本的访问控制列表 (ACL)	Read	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
GetObjectVersionTagging	授予权限以返回特定版本对象的标签集	Read	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
ListBucket	授予权限以列出 Amazon S3 存储桶中的部分或全部对象（最多 1000 个）	列出	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
ListBucketMultipartUploads	授予权限以列出正在进行的分段上传	列出	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
ListBucketVersions	授予权限以列出有关 Amazon S3 存储桶中所有对象版本的元数据	List	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
ListMultipartUploadParts	授予权限以列出为特定分段上传而上传的部分	List	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObject	授予权限以将对象添加到存储桶	写入	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectAcl	授予权限以便为 S3 存储桶中的新对象或现有对象设置访问控制列表（ACL）权限	权限管理	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectLegalHold	授予权限以将依法保留配置应用于指定的对象	写入	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectRetention	授予权限以在对象上放置对象保留配置	写入	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectTagging	授予权限以将提供的标签集设置为存储桶中已存在的对象	标记	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectVersionAcl	授予权限以使用 acl 子资源为存储桶中已存在的对象设置访问控制列表（ACL）权限	权限管理	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
PutObjectVersionTagging	授予权限以便为对象的特定版本设置提供的标签集	Tagging	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
RestoreObject	授予权限以将对象的归档副本恢复到 Amazon S3	写入	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
WriteGetObjectResponse	授予为发送到 S3 对象 Lambda 的 GetObject 请求提供数据的权限	写入	objectlambdaaccesspoint*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	

Amazon S3 Object Lambda 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
objectlambdaaccesspoint	`arn:${Partition}:s3-object-lambda:${Region}:${Account}:accesspoint/${AccessPointName}`	

Amazon S3 Object Lambda 的条件键

Amazon S3 Object Lambda 定义以下可以在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
s3-object-lambda:TlsVersion	按客户端使用的 TLS 版本筛选访问	数值
s3-object-lambda:authType	按身份验证方法筛选访问	字符串
s3-object-lambda:signatureAge	按请求签名的生存期（以毫秒为单位）筛选访问	数值
s3-object-lambda:versionid	按特定对象版本筛选访问权限	字符串

Amazon Savings Plans 的操作、资源和条件键

Amazon Savings Plans（服务前缀:savingsplans）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Savings Plans 定义的操作

- Amazon Savings Plans 定义的资源类型
- Amazon Savings Plans 的条件键

Amazon Savings Plans 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateSavingsPlan	授予权限以创建 Savings Plan	Write		aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteQueuedSavingsPlan	授予权限以删除与客户账户关联的已排队 Savings Plan	Write	savingsplan*		
				aws:ResourceTag/${TagKey}	
DescribeSavingsPlanRates	授予权限以描述与客户的 Savings Plan 相关的费率	Read	savingsplan*		
				aws:ResourceTag/${TagKey}	
DescribeSavingsPlans	授予权限以描述与客户账户关联的 Savings Plans	Read	savingsplan*		
				aws:ResourceTag/${TagKey}	
DescribeSavingsPlansOfferingRates	授予权限以描述与 Savings Plans 产品相关的费率	Read			
DescribeSavingsPlansOfferings	授予权限以描述客户有资格购买的 Savings Plans 产品	Read			
ListTagsForResource	授予权限以列出 Savings Plan 的标签	列表	savingsplan*		
ReturnSavingsPlan	授予权限以返回节省计划	写入	savingsplan*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey}	
TagResource	授予权限以标记 Savings Plan	Tagging	savingsplan*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	授予权限以取消标记 Savings Plan	Tagging	savingsplan*		
				aws:TagKeys	

Amazon Savings Plans 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
savingsplan	arn:${Partition}:savingsplans::${Account}:savingsplan/${ResourceId}	aws:ResourceTag/${TagKey}

Amazon Savings Plans 的条件键

Amazon Savings Plans 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按每个标签的允许值集筛选访问	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签值筛选访问权限	字符串
aws:TagKeys	按请求中是否具有必需标签来筛选访问	ArrayOfString

Amazon Secrets Manager 的操作、资源和条件键

Amazon Secrets Manager（服务前缀:secretsmanager）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Secrets Manager 定义的操作
- Amazon Secrets Manager 定义的资源类型
- Amazon Secrets Manager 的条件键

Amazon Secrets Manager 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchGetSecretValue	授予检索密钥列表并进行解密的权限	列表			
CancelRotateSecret	授予权限以取消进行中的密钥轮换	写入	Secret*		
				secretsmanager:SecretId	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
CreateSecret	授予权限以创建密钥，其中存储着可查询和轮换的加密数据	写入	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:Name secretsmanager:Description secretsmanager:KmsKeyArn secretsmanager:KmsKeyId aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys secretsmanager:ResourceTag/tag-key secretsmanager:Add	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				ReplicaRegions secretsmanager:ForceOverwriteReplicaSecret	
DeleteResourcePolicy	授予权限以删除附加到密钥的资源策略	权限管理	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteSecret	授予删除密钥的权限	写入	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:RecoveryWindowInDays secretsmanager:ForceDeleteWithoutRecovery secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:Sec	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				retPrimaryRegion	
DescribeSecret	授予权限以检索密钥的元数据，但不包含加密数据	读取	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
GetRandomPassword	授予权限以生成随机字符串以用于创建密码	读取			
GetResourcePolicy	授予权限以获取附加到密钥的资源策略	读取	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
GetSecretValue	授予权限以检索和解密加密数据	读取	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId secretsmanager:VersionId secretsmanager:VersionStage secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
ListSecretVersionIds	授予权限以列出可用的密钥版本	读取	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
ListSecrets	授予权限以列出可用密钥	列表			
PutResourcePolicy	授予将资源策略附加到密钥的权限	权限管理	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:BlockPublicPolicy secretsmanager:SecretPrimaryRegion	
PutSecretValue	授予权限以使用新的加密数据创建密钥的新版本	写入	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
RemoveRegionsFromReplication	授予权限以从复制中删除区域	写入	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
ReplicateSecretToRegions	授予权限以将现有密钥转换为多区域密钥，然后开始将该密钥复制到新区域的列表中	写入	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:AddReplicaRegions secretsmanager:ForceOverwri	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				teReplicaSecret	
RestoreSecret	授予取消删除密钥的权限	写入	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
RotateSecret	授予权限以启动轮换密钥	写入	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId secretsmanager:RotationLambdaARN secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:ModifyRotationRules	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:RotateImmediately	
StopReplicationToReplica	授予权限以从复制中删除密钥，并将该密钥提升为副本区域中的区域密钥	写入	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
TagResource	授予权限以将标签添加至密钥	标记	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId aws:RequestTag/${TagKey} aws:TagKeys secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
UntagResource	授予权限以从密钥中删除标签	标记	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId aws:TagKeys secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
UpdateSecret	授予权限以使用新的元数据或新版本的加密数据更新密钥	写入	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId secretsmanager:Description secretsmanager:KmsKeyArn secretsmanager:KmsKeyId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:Sec	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				retPrimaryRegion	
UpdateSecretVersionStage	授予权限以将阶段从一个密钥移动到另一个密钥	写入	Secret*		
				secretsmanager:SecretId secretsmanager:VersionStage secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ValidateResourcePolicy	授予权限以在附加策略之前验证资源策略	权限管理	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Amazon Secrets Manager 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
Secret	arn:${Partition}:secretsmanager:${Region}:${Account}:secret:${SecretId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys secretsmanager:ResourceTag/tag-key secretsmanager:resource/AllowRotationLambdaArn

Amazon Secrets Manager 的条件键

Amazon Secrets Manager 定义了以下可以在 IAM 策略Condition元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据用户向 Secrets Manager 服务发出的请求中的键筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	根据用户向 Secrets Manager 服务发出的请求中存在的所有标签键名称的列表筛选访问权限	ArrayOfString

条件键	描述	类型
secretsmanager:AddReplicaRegions	按要复制密钥的区域列表筛选访问权限	ArrayOfString
secretsmanager:BlockPublicPolicy	根据资源策略是否阻止广泛访问来筛选 Amazon Web Services 账户 访问权限	布尔型
secretsmanager:Description	根据请求中的描述文本筛选访问权限	字符串
secretsmanager:ForceDeleteWithoutRecovery	按是否在没有任何恢复时段的情况下立即删除密钥以筛选访问权限	布尔型
secretsmanager:ForceOverwriteReplicaSecret	根据是否覆盖目标区域中具有相同名称的密钥来筛选访问权限	布尔型
secretsmanager:KmsKeyArn	按请求中 KMS 密钥的密钥 ARN 筛选访问权限	ARN
secretsmanager:KmsKeyId	按请求中 KMS 密钥的密钥标识符筛选访问权限。已弃用：使用 secretsManager：KmsKeyArn	字符串
secretsmanager:ModifyRotationRules	按是否需要修改密钥轮换规则来筛选访问权限	布尔型
secretsmanager:Name	根据请求中易于识别的密钥名称筛选访问权限	字符串

条件键	描述	类型
secretsmanager:RecoveryWindowInDays	按 Secrets Manager 在删除密钥之前可以等待的天数筛选访问权限	数值
secretsmanager:ResourceTag/tag-key	按标签键值对筛选访问	字符串
secretsmanager:RotateImmediately	按是否需要立即轮换密钥来筛选访问权限	布尔型
secretsmanager:RotationLambdaARN	根据请求中轮换 Lambda 函数的 ARN 筛选访问权限	ARN
secretsmanager:SecretId	根据请求中的 SecretID 值筛选访问权限	ARN
secretsmanager:SecretPrimaryRegion	根据在其中创建密钥的主要区域筛选访问权限	字符串
secretsmanager:VersionId	根据请求中密钥版本的唯一标识符筛选访问权限	字符串
secretsmanager:VersionStage	根据请求中的版本阶段列表筛选访问权限	字符串

条件键	描述	类型
secretsmanager:resource/AllowRotationLambdaArn	根据与密钥关联的轮换 Lambda 函数的 ARN 筛选访问权限	ARN

Amazon Security Hub 的操作、资源和条件键

Amazon Security Hub（服务前缀:`securityhub`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Security Hub 定义的操作
- Amazon Security Hub 定义的资源类型
- Amazon Security Hub 的条件键

Amazon Security Hub 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AcceptAdministratorInvitation	授予权限以接受成为成员账户的 Security Hub 邀请	Write	hub		
AcceptInvitation	授予权限以接受成为成员账户的 Security Hub 邀请	写入	hub		
BatchDeleteAutomationRules	授予权限以删除 Security Hub 中的一个或多个自动化规则	写入	automation-rule*		
BatchDisableStandards	授予权限以在 Security Hub 中禁用标准	Write	hub		
BatchEnableStandards	授予权限以在 Security Hub 中启用标准	写入	hub		
BatchGetAutomationRules	根据规则 Amazon 资源名称 (ARNs) 授予从 Security Hub 检索自动化规则详情列表的权限	读取	automation-rule*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchGetConfigurationPolicyAssociations	授予检索与调用账户所在组织的特定成员账户列表和组织单位关联的配置策略信息的权限	读取			
BatchGetControlEvaluations[仅权限]	授予权限以获取控件的启用和合规性状态、控件的调查发现计数以及 Security Hub 控制台上控件的总体安全性评分	读取	hub		
BatchGetSecurityControls	授予权限以获取通过 ID 或 ARN 标识的特定安全控件的详细信息	读取			securityhub:DescribeStandardsControls
BatchGetStandardsControlAssociations	授予权限以获取标准中一批安全控件的启用状态	读取			securityhub:DescribeStandardsControls
BatchImportFindings	授予权限以将结果从集成产品导入 Security Hub	写入	product*		
				securityhub:TargetAccount	
BatchUpdateAutomationRules	根据规则 Amazon 资源名称 (ARNs) 和输入参数授予从 Security Hub 更新一条或多条自动化规则的权限	写入	automation-rule*		
BatchUpdateFindings		写入	hub		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
	授予权限以更新一组选定的 Security Hub 结果的客户控制字段			securityhub:ASFFSyntaxPath/${ASFFSyntaxPath}	
BatchUpdateStandardsControlAssociations	授予权限以更新标准中一批安全控件的启用状态	写入			securityhub:UpdateStandardsControl
CreateActionTarget	授予权限以在 Security Hub 中创建自定义操作	写入	hub		
CreateAutomationRule	授予权限以基于输入参数创建自动化规则	写入		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfigurationPolicy	授予在 Security Hub 中创建配置策略以管理组织成员设置的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFindingAggregator	授予权限以创建结果聚合器，其中包含跨区域结果聚合配置	写入			
CreateInsight	授予权限以在 Security Hub 中创建洞察。洞察是相关结果的集合	Write	hub		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateMembers	授予权限以在 Security Hub 中创建成员账户	Write	hub		
DeclineInvitations	授予权限以拒绝成为成员账户的 Security Hub 邀请	Write	hub		
DeleteActionTarget	授予权限以删除 Security Hub 中的自定义操作	写入	hub		
DeleteConfigurationPolicy	授予删除现有配置策略的权限	写入	configuration-policy*		
DeleteFindingAggregator	授予权限以删除结果聚合器，这将禁用跨区域结果聚合	写入	finding-aggregator*		
DeleteInsight	授予权限以从 Security Hub 中删除洞察	Write	hub		
DeleteInvitations	授予权限以删除成为成员账户的 Security Hub 邀请	Write	hub		
DeleteMembers	授予权限以删除 Security Hub 成员账户	Write	hub		
DescribeActionTargets	授予权限以使用 API 检索自定义操作列表	Read	hub		
DescribeHub	授予权限以检索有关您的账户中的 Hub 资源的信息	Read	hub		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeOrganizationConfiguration	授予描述 Security Hub 组织配置的权限	Read	hub		
DescribeProducts	授予权限以检索有关可用 Security Hub 产品集成的信息	Read	hub		
DescribeStandards	授予权限以检索有关 Security Hub 标准的信息	Read	hub		
DescribeStandardsControls	授予权限以检索有关 Security Hub 标准控件的信息	Read	hub		
DisableImportFindingsForProduct	授予权限以禁用 Security Hub 集成产品的结果导入	Write	hub		
DisableOrganizationAdminAccount	授予删除组织的 Security Hub 管理员帐户的权限	Write	hub		organizations:DescribeOrganization
DisableSecurityHub	授予权限以禁用 Security Hub	Write	hub		
DisassociateFromAdministratorAccount	授予 Security Hub 成员账户从关联的管理员账户中取消关联的权限	Write	hub		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DisassociateFromMasterAccount	授予对 Security Hub 成员账户的权限以从关联的主账户中取消关联	Write	hub		
DisassociateMembers	授予从关联的管理员账户中取消关联 Security Hub 成员账户的权限	Write	hub		
EnableImportFindingsForProduct	授予权限以启用 Security Hub 集成产品的结果导入	Write	hub		
EnableOrganizationAdminAccount	授予指定组织的 Security Hub 管理员帐户的权限	Write	hub		organizations:DescribeOrganization organizations:EnableAWSServiceAccess organizations:RegisterDelegatedAdministrator
EnableSecurityHub	授予权限以启用 Security Hub	Write	hub		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
GetAdhocInsightResults[仅权限]	授予权限以通过提供一组筛选器（而不是洞察 ARN）检索洞察结果	Read	hub		
GetAdministratorAccount	授予权限以检索有关 Security Hub 管理员账户的详细信息	读取	hub		
GetConfigurationPolicy	授予获取调用账户所创建一项配置策略的完整概览的权限	读取	configuration-policy*		
GetConfigurationPolicyAssociation	授予检索与调用账户所在组织的某个成员账户或组织单位关联的某个配置策略信息的权限	读取			
GetControlFindingSummary[仅权限]	授予检索安全评分以及安全标准状态的调查结果计数和控件状态的权限	Read	hub		
GetEnabledStandards	授予权限以检索在 Security Hub 中启用的标准列表	列表	hub		
GetFindingAggregator	授予权限以检索结果聚合器的详细信息，这将配置跨区域结果聚合	读取	finding-aggregator*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetFindingHistory	授予权限以从 Security Hub 检索调查发现历史记录的列表	读取	hub		
GetFindings	授予权限以从 Security Hub 检索结果的列表	Read	hub		
GetFreeTrialEndDate[仅权限]	授予权限以检索账户免费试用 Security Hub 的结束日期	Read	hub		
GetFreeTrialUsage[仅权限]	授予权限以检索免费试用期内 Security Hub 使用情况的信息	Read	hub		
GetInsightFindingTrend[仅权限]	授予权限以从 Security Hub 检索洞察发现趋势，从而生成图表	Read	hub		
GetInsightResults	授予权限以从 Security Hub 检索洞察结果	Read	hub		
GetInsights	授予权限以检索 Security Hub 洞察	List	hub		
GetInvitationsCount	授予权限以检索发送到账户的 Security Hub 成员资格邀请的计数	Read	hub		
GetMasterAccount	授予权限以检索有关 Security Hub 主账户的详细信息	Read	hub		
GetMembers	授予权限以检索 Security Hub 成员账户的详细信息	读取	hub		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetSecurityControlDefinition	授予获取用 ID 标识的特定安全控件详细信息的权限	读取			securityhub:DescribeStandardsControls
GetUsage[仅权限]	授予权限以按账户检索有关 Security Hub 使用情况的信息	读取	hub		
InviteMembers	授予邀请其他 Amazon 账户成为 Security Hub 成员账户的权限	写入	hub		
ListAutomationRules	授予权限以从 Security Hub 检索呼叫账户的自动化规则列表及其元数据	列表			
ListConfigurationPolicies	授予列出调用账户所创建所有配置策略的摘要的权限	列表			
ListConfigurationPolicyAssociations	授予检索与调用账户所在组织的所有成员账户和组织单位关联的所有配置策略信息的权限	列表			
ListControlEvaluationSummaries[仅权限]	授予检索标准控件列表的权限，包括控件 IDs、状态和查找次数	读取	hub		
ListEnabledProductsForImport	授予权限以检索当前启用的 Security Hub 集成产品	列表	hub		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListFindingAggregators	授予权限以检索结果聚合器的列表，其中包含跨区域结果聚合配置	列表			
ListInvitations	授予权限以检索发送到账户的 Security Hub 邀请	List	hub		
ListMembers	授予权限以检索与管理员账户关联的 Security Hub 成员账户的详细信息	List	hub		
ListOrganizationAdminAccounts	授予列出组织的 Security Hub 管理员帐户的权限	列表	hub		organizations:DescribeOrganization
ListSecurityControlDefinitions	授予权限以检索安全控件定义列表，其中包含当前区域中安全控件的详细信息	列表			
ListStandardsControlAssociations	授予权限以列出标准中安全控件的启用状态	列表			securityhub:DescribeStandardsControls
ListTagsForResource	授予权限以列出与资源关联的标签	Read	automation-rule		
			configuration-policy		
			hub		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
SendFindingEvents[仅权限]	授予使用自定义操作向亚马逊发送 Security Hub 调查结果的权限 EventBridge	读取	hub		
SendInsightEvents[仅权限]	授予使用自定义操作向亚马逊发送 Security Hub 见解的权限 EventBridge	读取	hub		
StartConfigurationPolicyAssociation	授予将某个配置策略关联到调用账户所在组织的某个成员账户或组织单位的权限	写入	configuration-policy		
StartConfigurationPolicyDisassociation	授予从调用账户所在组织的某个成员账户或组织单位移除某个配置策略的权限	写入	configuration-policy		
TagResource	授予权限以将标签添加到 Security Hub 资源	Tagging	automation-rule		
			configuration-policy		
			hub		
UntagResource	授予权限以从 Security Hub 资源中删除标签	Tagging	automation-rule		
			configuration-policy		
			hub		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateActionTarget	授予权限以在 Security Hub 中更新自定义操作	写入	hub		
UpdateConfigurationPolicy	授予更新现有配置策略的权限	写入	configuration-policy*		
UpdateFindingAggregator	授予权限以更新结果聚合器，其中包含跨区域结果聚合配置	写入	finding-aggregator*		
UpdateFindings	授予权限以更新 Security Hub 结果	Write	hub		
UpdateInsight	授予权限以在 Security Hub 中更新洞察	Write	hub		
UpdateOrganizationConfiguration	授予更新 Security Hub 组织配置的权限	写入	hub		
UpdateSecurityControl	授予更新用 ID 或 ARN 标识的特定安全控件的属性的权限	写入			securityhub:UpdateStandardsControl
UpdateSecurityHubConfiguration	授予权限以更新 Security Hub 配置	Write	hub		
UpdateStandardsControl	授予权限以更新 Security Hub 标准控件	Write	hub		

Amazon Security Hub 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
hub	arn:${Partition}:securityhub:${Region}:${Account}:hub/default	aws:ResourceTag/${TagKey}
product	arn:${Partition}:securityhub:${Region}:${Account}:product/${Company}/${ProductId}	
finding-aggregator	arn:${Partition}:securityhub:${Region}:${Account}:finding-aggregator/${FindingAggregatorId}	
automation-rule	arn:${Partition}:securityhub:${Region}:${Account}:automation-rule/${AutomationRuleId}	
configuration-policy	arn:${Partition}:securityhub:${Region}:${Account}:configuration-policy/${ConfigurationPolicyId}	

Amazon Security Hub 的条件键

Amazon Security Hub 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中是否具有标签键值对来按照操作筛选访问权限	字符串
aws:ResourceTag/${TagKey}	根据附加到资源的标签键值对来按操作筛选访问权限	字符串
aws:TagKeys	根据在请求中是否具有标签键来按操作筛选访问权限	ArrayOfString
securityhub:ASFFSyntaxPath/${ASFFSyntaxPath}	根据请求中的指定字段和值筛选访问权限	字符串
securityhub:TargetAccount	按请求中指定的 AwsAccountId 字段筛选访问权限	字符串

Amazon Server Migration Service 的操作、资源和条件键

Amazon 服务器迁移服务（服务前缀:sms）提供以下特定于服务的资源、操作和条件上下文密钥，用于 IAM 权限策略。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Server Migration Service 定义的操作
- Amazon Server Migration Service 定义的资源类型
- Amazon Server Migration Service 的条件键

Amazon Server Migration Service 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateApp	授予创建应用程序配置以将本地应用程序迁移到的权限 Amazon	写入			
CreateReplicationJob	授予创建任务以将本地服务器迁移到的权限 Amazon	写入			
DeleteApp	授予权限以删除现有应用程序配置	Write			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteAppLaunchConfiguration	授予权限以删除现有应用程序的启动配置	Write			
DeleteAppReplicationConfiguration	授予权限以删除现有应用程序的复制配置	Write			
DeleteAppValidationConfiguration	授予权限以删除现有应用程序的验证配置	写入			
DeleteReplicationJob	授予删除现有任务以将本地服务器迁移到的权限 Amazon	写入			
DeleteServerCatalog	授予删除收集到的本地服务器完整列表的权限 Amazon	写入			
DisassociateConnector	授予权限以取消关联已关联的连接器	写入			
GenerateChangeSet	授予为应用程序堆栈生成变更集 CloudFormation 的权限	写入			
GenerateTemplate	授予为现有应用程序生成 CloudFormation 模板的权限	写入			
GetApp	授予权限以获取现有应用程序的配置和状态	Read			
GetAppLaunchConfiguration	授予权限以获取现有应用程序的启动配置	Read			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetAppReplicationConfiguration	授予权限以获取现有应用程序的复制配置	Read			
GetAppValidationConfiguration	授予权限以获取现有应用程序的验证配置	Read			
GetAppValidationOutput	授予权限以从应用程序验证脚本获取发送的通知。	Read			
GetConnectors	授予权限以获取已关联的所有连接器	读取			
GetMessages [仅权限]	授予将消息从 Amazon 服务器迁移服务发送到服务器迁移连接器的权限	读取			
GetReplicationJobs	授予将所有现有任务迁移到本地服务器的权限 Amazon	读取			
GetReplicationRuns	授予权限以获取现有作业的所有运行	Read			
GetServers	授予权限以获取已导入的所有服务器	读取			
ImportAppCatalog	授予从 Application Discovery Service 导入 Amazon 应用程序目录的权限	写入			
ImportServerCatalog	授予权限以收集本地服务器的完整列表	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
LaunchApp	授予为现有应用程序创建和启动 CloudFormation 堆栈的权限	写入			
ListApps	授予权限以获取现有应用程序的摘要列表	List			
NotifyAppValidationOutput	授予权限以发送应用程序验证脚本的通知	Write			
PutAppLaunchConfiguration	授予权限以为现有的应用程序创建或更新启动配置	Write			
PutAppReplicationConfiguration	授予权限以为现有的应用程序创建或更新复制配置	Write			
PutAppValidationConfiguration	授予权限以对现有应用程序放置验证配置	写入			
SendMessage [仅权限]	授予从服务器迁移连接器向 Amazon 服务器迁移服务发送消息的权限	写入			
StartAppReplication	授予权限以便为现有应用程序创建和启动复制作业	Write			
StartOnDemandAppReplication	授予权限以对现有应用程序启动复制运行	Write			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StartOnDemandReplicationRun	授予权限以对现有复制作业启动复制运行	Write			
StopAppReplication	授予权限以停止和删除现有应用程序的复制作业	写入			
TerminateApp	授予终止现有应用程序 CloudFormation 堆栈的权限	写入			
UpdateApp	授予权限以更新现有应用程序配置	写入			
UpdateReplicationJob	授予更新现有任务以将本地服务器迁移到的权限 Amazon	写入			

Amazon Server Migration Service 定义的资源类型

Amazon 服务器迁移服务不支持在 IAM 策略声明的`Resource`元素中指定资源 ARN。要允许对 Amazon Server Migration Service 的访问权限，请在策略中指定 `"Resource": "*"`。

Amazon Server Migration Service 的条件键

ServerMigrationService 没有可在策略声明`Condition`元素中使用的特定于服务的上下文密钥。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon Serverless Application Repository 的操作、资源和条件键

Amazon Serverless Application Repository（服务前缀`serverlessrepo:`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。

- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Serverless Application Repository 定义的操作
- Amazon Serverless Application Repository 定义的资源类型
- Amazon Serverless Application Repository 的条件键

Amazon Serverless Application Repository 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateApplication	授予创建应用程序的权限，可以选择包括一个 Amazon SAM 文件，以便在同一次调用中创建第一个应用程序版本	写入			
CreateApplicationVersion	授予创建应用程序版本的权限	写入	applications*		
CreateCloudFormationChangeSet	授予为给定应用程序创建的权限 Amazon CloudFormation ChangeSet	写入	applications*		
				serverlessrepo:applicationType	
CreateCloudFormationTemplate	授予创建 Amazon CloudFormation 模板的权限	写入	applications*		
				serverlessrepo:applicationType	
DeleteApplication	授予删除指定应用程序的权限	写入	applications*		
GetApplication	授予获取指定应用程序的权限	读取	applications*		
				serverlessrepo:app	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				licationType	
GetApplicationPolicy	授予获取指定应用程序策略的权限	读取	applications*		
GetCloudFormationTemplate	授予获取指定 Amazon CloudFormation 模板的权限	读取	applications*		
ListApplicationDependencies	授予检索包含应用程序中嵌套的应用程序列表的权限	列表	applications*		
				serverlessrepo:applicationType	
ListApplicationVersions	授予列出请求者所拥有的指定应用程序版本的权限	列表	applications*		
				serverlessrepo:applicationType	
ListApplications	授予列出请求者所拥有应用程序的权限	列表			
PutApplicationPolicy	授予为指定应用程序放置策略的权限	写入	applications*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
SearchApplications	授予获取为此用户授权的所有应用程序的权限	读取		serverlessrepo:applicationType	
UnshareApplication	授予取消共享指定应用程序的权限	写入	applications*		
UpdateApplication	授予更新应用程序元数据的权限	写入	applications*		

Amazon Serverless Application Repository 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
applications	`arn:${Partition}:serverlessrepo:${Region}:${Account}:applications/${ResourceId}`	

Amazon Serverless Application Repository 的条件键

Amazon Serverless Application Repository 定义了以下可以在 IAM 策略元素中Condition使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
serverlessrepo:applicationType	按应用程序类型筛选访问权限	字符串

Service Quotas 的操作、资源和条件键

Service Quotas（服务前缀：servicequotas）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Service Quotas 定义的操作
- Service Quotas 定义的资源类型
- Service Quotas 的条件键

Service Quotas 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateServiceQuotaTemplate	授予权限以将 Service Quotas 模板与您的组织相关联	Write			organizations:DescribeOrganization organizations:EnableAWSServiceAccess
DeleteServiceQuotaIncreaseRequestFromTemplate	授予权限以从服务配额模板中删除指定的服务配额	Write			organizations:DescribeOrganization
DisassociateServiceQuotaTemplate	授予权限以将 Service Quotas 模板与您的组织取消关联	写入			organizations:DescribeOrganization

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetAWSDefaultServiceQuota	授予返回指定服务配额详细信息的权限，包括 Amazon 默认值	读取			
GetAssociationForServiceQuotaTemplate	授予检索该 ServiceQuotaTemplateAssociationStatus 值的权限，该值会告诉你 Service Quotas 模板是否与组织关联	读取			organizations:DescribeOrganization
GetRequestedServiceQuotaChange	授予权限以检索特定服务配额增加请求的详细信息	Read			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetServiceQuota	授予权限以返回指定服务配额的详细信息，包括应用的值	Read			autoscaling:DescribeAccountLimits cloudformation:DescribeAccountLimits dynamodb:DescribeLimits elasticloadbalancing:DescribeAccountLimits iam:GetAccountSummary kinesis:DescribeLimits rds:DescribeAccountAttributes

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
					route53:GetAccountLimit
GetServiceQuotaIncreaseRequestFromTemplate	授予权限以从服务配额模板中检索服务配额增加请求的详细信息	读取			organizations:DescribeOrganization
ListAWSDefaultServiceQuotas	授予列出指定 Amazon 服务的所有默认服务配额的权限	读取			
ListRequestedServiceQuotaChangeHistory	授予权限以请求服务配额的更改列表	Read			
ListRequestedServiceQuotaChangeHistoryByQuota	授予权限以请求特定服务配额的更改列表	Read			
ListServiceQuotaIncreaseRequestsInTemplate	授予权限以从服务配额模板中返回服务配额增加请求列表	读取			organizations:DescribeOrganization

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListServiceQuotas	授予列出该账户、该区域中指定 Amazon 服务的所有服务配额的权限	读取			autoscaling:DescribeAccountLimits cloudformation:DescribeAccountLimits dynamodb:DescribeLimits elasticloadbalancing:DescribeAccountLimits iam:GetAccountSummary kinesis:DescribeLimits rds:DescribeAccountAttributes

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
					route53:GetAccountLimit
ListServices	授予在 Service Quotas 中列出可用 Amazon 服务的权限	读取			
ListTagsForResource	授予查看 SQ 资源上现有标签的权限	读取			
PutServiceQuotaIncreaseRequestIntoTemplate	授予权限以定义配额，并将其添加到服务配额模板中	Write	quota		organizations:DescribeOrganization
				servicequotas:service	
RequestServiceQuotaIncrease	授予权限以提交服务配额增加请求	Write	quota		
				servicequotas:service	
TagResource	授予将一组标签与现有 SQ 资源关联的权限	Tagging		aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UntagResource	授予从 SQ 资源中删除一组标签的权限（其中要删除的标签与一组客户提供的标签键匹配）	Tagging		aws:TagKeys	

Service Quotas 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
quota	arn:${Partition}:servicequotas:${Region}:${Account}:${ServiceCode}/${QuotaCode}	

Service Quotas 的条件键

Service Quotas 定义以下可以在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串

条件键	描述	类型
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString
servicequotas:service	筛选指定 Amazon 服务的访问权限	字符串

Amazon Signer 的操作、资源和条件键

Amazon Signer（服务前缀:`signer`）提供以下特定于服务的资源、操作和条件上下文密钥，以用于 IAM 权限策略。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Signer 定义的操作
- Amazon Signer 定义的资源类型
- Amazon Signer 的条件键

Amazon Signer 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须

具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddProfilePermission	授予向签名配置文件添加跨账户权限的权限	Permissions management	signing-profile*		
CancelSigningProfile	授予将签名配置文件的状态更改为 CANCELED 的权限	Write	signing-profile*		
				signer:ProfileVersion	
DescribeSigningJob	授予返回有关特定签名作业信息的权限	读取	signing-job*		
GetRevocationStatus	授予权限以查询签名资源的撤销信息	读取	signing-job*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			signing-profile*		
GetSigningPlatform	授予返回有关特定签名平台信息的权限	Read			
GetSigningProfile	授予返回有关特定签名配置文件信息的权限	Read	signing-profile*		
				signer:ProfileVersion	
ListProfilePermissions	授予列出与签名配置文件关联的跨账户权限的权限	Read	signing-profile*		
ListSigningJobs	授予列出账户中所有签名作业的权限	List			
ListSigningPlatforms	授予列出所有可用的签名平台的权限	List			
ListSigningProfiles	授予列出账户中所有签名配置文件的权限	List			
ListTagsForResource	授予列出与 Signing Profile 关联的标签的权限	Read	signing-profile*		
PutSigningProfile	授予创建新签名配置文件的权限	Write		aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
RemoveProfilePermission	授予从签名配置文件中删除跨账户权限的权限	Permissions management	signing-profile*		
RevokeSignature	授予将签名作业状态更改为 REVOKED 的权限	Write	signing-job*		
				signer:ProfileVersion	
RevokeSigningProfile	授予将签名配置文件状态更改为 REVOKED 的权限	写入	signing-profile*		
				signer:ProfileVersion	
SignPayload	授予权限以对提供的负载启动签名作业	写入	signing-profile*		
				signer:ProfileVersion	
StartSigningJob	授予对提供的代码启动签名作业的权限	Write	signing-profile*		
				signer:ProfileVersion	
TagResource	授予向签名配置文件添加一个或多个标签的权限	Tagging	signing-profile*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	授予从 Signing Profile 删除一个或多个标签的权限	Tagging	signing-profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Amazon Signer 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
signing-profile	arn:${Partition}:signer:${Region}:${Account}:/signing-profiles/${ProfileName}	aws:ResourceTag/${TagKey}
signing-job	arn:${Partition}:signer:${Region}:${Account}:/signing-jobs/${JobId}	

Amazon Signer 的条件键

Amazon 签名者定义了以下条件密钥，这些条件密钥可用于 IAM 策略的Condition元素中。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按每个标签的允许值集筛选访问	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签值筛选访问权限	字符串
aws:TagKeys	按请求中是否具有必需标签来筛选访问	ArrayOfString
signer:ProfileVersion	根据签名配置文件的版本筛选访问	字符串

Amazon Simple Workflow Service 的操作、资源和条件键

Amazon Simple Workflow Service（服务前缀：swf）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Simple Workflow Service 定义的操作
- Amazon Simple Workflow Service 定义的资源类型
- Amazon Simple Workflow Service 的条件键

Amazon Simple Workflow Service 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CancelTimer[仅权限]	授予取消先前启动的计时器并在历史记录中记录 TimerCanceled 事件的权限	写入	domain*		
CancelWorkflowExecution[仅权限]	授予关闭工作流程执行并在历史记录中记录 WorkflowExecutionCanceled 事件的权限	写入	domain*		
CompleteWorkflowEx	授予关闭工作流程执行并在历史记录中记录 WorkflowE	写入	domain*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ecution[仅权限]	xecutionCompleted 事件的权限				
ContinueAsNewWorkflowExecution[仅权限]	授予权限以关闭工作流程执行并使用相同工作流 ID 和唯一运行 ID 启动相同类型的新工作流程执行	写入	domain*		
CountClosedWorkflowExecutions	授予权限以返回在给定域中满足指定筛选条件的已关闭工作流程执行数	读取	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	
CountOpenWorkflowExecutions	授予权限以返回在给定域中满足指定筛选条件的已开启工作流程执行数	读取	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	
	授予权限以返回指定任务列表中的活动任务的估计数量	读取	domain*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CountPendingActivityTasks				swf:taskList.name	
CountPendingDecisionTasks	授予权限以返回指定任务列表中的决策任务的估计数量	读取	domain*		
				swf:taskList.name	
DeleteActivityType	授予权限以删除指定活动类型	写入	domain*		
				swf:activityType.name swf:activityType.version	
DeleteWorkflowType	授予权限以删除指定工作流类型	写入	domain*		
				swf:workflowType.name swf:workflowType.version	
DeprecateActivityType	授予权限以弃用指定活动类型	写入	domain*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				swf:activityType.name swf:activityType.version	
DeprecateDomain	授予权限以弃用指定域	写入	domain*		
DeprecateWorkflowType	授予权限以弃用指定工作流类型	写入	domain*		
				swf:workflowType.name swf:workflowType.version	
DescribeActivityType	授予权限以返回指定活动类型	读取	domain*		
				swf:activityType.name swf:activityType.version	
DescribeDomain	授予权限以返回有关指定域的信息，包括其描述和状态	读取	domain*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeWorkflowExecution	授予权限以返回有关指定工作流程执行的信息，包括其类型和一些统计数据	读取	domain*		
DescribeWorkflowType	授予权限以返回指定工作流类型	读取	domain*		
				swf:workflowType.name swf:workflowType.version	
FailWorkflowExecution[仅权限]	授予关闭工作流程执行并在历史记录中记录 WorkflowExecutionFailed 事件的权限	写入	domain*		
GetWorkflowExecutionHistory	授予权限以返回指定工作流执行的历史记录	读取	domain*		
ListActivityTypes	授予权限以返回在指定域中注册的与指定名称和注册状态匹配的所有活动的相关信息	列表	domain*		
ListClosedWorkflowExecutions	授予权限以返回在指定域中满足筛选条件的已关闭工作流程执行的列表	列表	domain*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	
ListDomains	授予权限以返回当前账户中注册的域列表	列表			
ListOpenWorkflowExecutions	授予权限以返回在指定域中满足筛选条件的已开启工作流执行的列表	列表	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	
ListTagsForResource	授予列出 Amazon SWF 资源标签的权限	列表	domain		
ListWorkflowTypes	授予权限以返回指定域中工作流类型的信息	列表	domain*		
PollForActivityTask	向工作人员授予 ActivityTask 从指定活动任务列表中获取的权限	写入	domain*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				swf:taskList.name	
PollForDecisionTask	允许决策者 DecisionTask 从指定的决策任务列表中获取	写入	domain*		
				swf:taskList.name	
RecordActivityTaskHeartbeat	允许工作人员向服务报告由指定 taskToken ActivityTask 表示的仍在进行中	写入	domain*		
RecordMarker[仅权限]	授予在历史记录中记录 MarkerRecorded 事件的权限	写入	domain*		
RegisterActivityType	授予权限以在指定域中注册新活动类型及其配置设置	写入	domain*		
				swf:defaultTaskList.name swf:name swf:version	
RegisterDomain	授予权限以注册新域	写入		aws:TagKeys aws:RequestTag/${TagKey}	
RegisterWorkflowType	授予权限以在指定域中注册新工作流类型及其配置设置	写入	domain*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				swf:defaultTaskList.name swf:name swf:version	
RequestCancelActivityTask[仅权限]	授予权限以尝试取消之前计划的活动任务	写入	domain*		
RequestCancelExternalWorkflowExecution[仅权限]	授予权限以请求取消指定的外部工作流执行的请求	写入	domain*		
RequestCancelWorkflowExecution	授予在由给定域 workFlowID 和 runID 标识的当前正在运行的工作流程执行中记录 WorkflowExecutionCancelRequested 事件的权限	写入	domain*		
RespondActivityTaskCanceled	允许工作人员告知服务 TaskToken 所 ActivityTask 识别的已成功取消	写入	domain*		
RespondActivityTaskCompleted	允许工作人员告知服务由 taskToken ActivityTask 标识的已成功完成并获得结果（如果提供）	写入	domain*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				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 swf:workflowType.name	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				swf:workflowType.version	
RespondActivityTaskFailed	允许工作人员告知服务由 taskToken ActivityTask 标识的失败原因已失败（如果已指定）	写入	domain*		
RespondDecisionTaskCompleted	向决策者授予权限，让他们告知服务由 taskToken DecisionTask 标识的已成功完成	写入	domain*		
ScheduleActivityTask[仅权限]	授予权限以安排活动任务	写入	domain*		
SignalExternalWorkflowExecution[仅权限]	授予权限以请求使信号提交至指定外部工作流执行和记录	写入	domain*		
SignalWorkflowExecution	授予在工作流程执行历史记录中记录 WorkflowExecutionSignaled 事件的权限，并为由给定域 workFlowID 和 runID 标识的工作流程执行创建决策任务	写入	domain*		
StartChildWorkflowExecution[仅权限]	授予权限以请求启动子工作流执行	写入	domain*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StartTimer[仅权限]	授予权限以启动工作流执行的计时	写入	domain*		
StartWorkflowExecution	授予权限以使用提供的 workflowId 和输入数据在指定域中启动工作流类型执行	写入	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	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
TagResource	授予标记 S Amazon WF 资源的权限	标记	domain		
				aws:TagKeys aws:RequestTag/${TagKey}	
TerminateWorkflowExecution	授予记录 WorkflowExecutionTerminated 事件并强制关闭由给定域、runID 和 WorkFlowID 标识的工作流程执行的权限	写入	domain*		
UndeprecateActivityType	授予权限以不建议使用先前已弃用的活动类型	写入	domain*		
				swf:activityType.name swf:activityType.version	
UndeprecateDomain	授予权限以不建议使用先前已弃用的域	写入	domain*		
UndeprecateWorkflowType	授予权限以不建议使用先前已弃用的工作流类型	写入	domain*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				swf:workflowType.name swf:workflowType.version	
UntagResource	授予从 Amazon SWF 资源中移除标签的权限	标记	domain		
				aws:TagKeys	

Amazon Simple Workflow Service 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
domain	arn:${Partition}:swf::${Account}:/domain/${DomainName}	aws:ResourceTag/${TagKey}

Amazon Simple Workflow Service 的条件键

Amazon Simple Workflow Service 定义以下可以在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按资源的标签筛选访问权限	字符串
aws:TagKeys	按键的标签筛选访问权限	ArrayOfString
swf:activityType.name	按活动类型的名称筛选访问权限	字符串
swf:activityType.version	按活动类型的版本筛选访问权限	字符串
swf:defaultTaskList.name	按默认任务列表的名称筛选访问权限	字符串
swf:name	按活动或工作流名称筛选访问	字符串
swf:tagFilter.tag	按 tagFilter.tag 值筛选访问权限	字符串
swf:tagList.member.0	按指定的标签筛选访问权限	字符串
swf:tagList.member.1	按指定的标签筛选访问权限	字符串
swf:tagList.member.2	按指定的标签筛选访问权限	字符串
swf:tagList.member.3	按指定的标签筛选访问权限	字符串
swf:tagList.member.4	按指定的标签筛选访问权限	字符串

条件键	描述	类型
swf:taskList.name	按任务列表的名称筛选访问权限	字符串
swf:typeFilter.name	按类型筛选条件的名称筛选访问权限	字符串
swf:typeFilter.version	按类型筛选条件的版本筛选访问权限	字符串
swf:version	按活动或工作流名称筛选访问权限	字符串
swf:workflowType.name	按工作流类型的名称筛选访问权限	字符串
swf:workflowType.version	按工作流类型的版本筛选访问权限	字符串

Amazon SimpleDB 的操作、资源和条件键

Amazon SimpleDB（服务前缀：sdb）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon SimpleDB 定义的操作
- Amazon SimpleDB 定义的资源类型
- Amazon SimpleDB 的条件键

Amazon SimpleDB 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchDeleteAttributes	在一次呼叫中执行多项 DeleteAttributes 操作，从而减少往返和延迟	写入	domain*		
BatchPutAttributes	通过该 BatchPutAttributes 操作，您可以在一次调用中执行多个 PutAttribute 操作。通过该 BatchPutAttributes 操作，	写入	domain*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
	您可以在一次调用中执行多个 PutAttribute 操作				
CreateDomain	该 CreateDomain 操作创建了一个新域	写入	domain*		
DeleteAttributes	删除与项目关联的一个或多个属性	写入	domain*		
DeleteDomain	该 DeleteDomain 操作会删除一个域	写入	domain*		
DomainMetadata	返回有关域的信息，包括域的创建时间、项目和属性的数量以及属性名称和值的大小	读取	domain*		
GetAttributes	返回与项目关联的所有属性	读取	domain*		
ListDomains	的描述 ListDomains	列表			
PutAttributes	该 PutAttributes 操作在项目中创建或替换属性	写入	domain*		
Select	Select 的描述	Read	domain*		

Amazon SimpleDB 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
domain	arn:${Partition}:sdb:${Region}:${Account}:domain/${DomainName}	

Amazon SimpleDB 的条件键

SimpleDB 没有可以在策略语句的 Condition 元素中使用的服务特定上下文键。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon Snowball 的操作、资源和条件键

Amazon Snowball（服务前缀:snowball）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Snowball 定义的操作
- Amazon Snowball 定义的资源类型
- Amazon Snowball 的条件键

Amazon Snowball 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须

具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CancelCluster	授予权限以取消集群任务	写入			
CancelJob	授予权限以取消指定任务	写入			
CreateAddress	授予权限以创建 Snowball 要发运到的地址	写入			
CreateCluster	授予权限以创建空集群	写入			
CreateJob	授予权限以创建在 Amazon S3 和您的本地数据中心之间导入或导出数据的任务	写入			
CreateLongTermPricing	授予创建权限以允许客户 LongTermPricingListEntry 为任务添加预付账单合同	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateReturnShippingLabel	授予创建发货标签的权限，该标签将用于将 Snow 设备退回 Amazon	写入			
DescribeAddress	授予权限以采用地址对象形式获取有关该地址的特定详细信息	读取			
DescribeAddresses	授予权限以描述指定数量的地址对象	列表			
DescribeCluster	授予权限以描述有关特定集群的信息，包括发运信息、集群状态和其他重要元数据	读取			
DescribeJob	授予权限以描述有关特定任务的信息，包括发运信息、任务状态和其他重要元数据	读取			
DescribeReturnShippingLabel	授予在要退回的 Snow 设备的运输标签上描述信息的权限 Amazon	读取			
GetJobManifest	授予权限以获取指向与指定值 JobId 关联的清单文件的 Amazon S3 预签名 URL 的链接	读取			
GetJobUnlockCode	授予获取指定作业 UnlockCode 代码值的权限	读取			
GetSnowballUsage	授予权限以获取有关您的账户的 Snowball 服务限制的信息，以及您的账户已使用的 Snowball 数量	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetSoftwareUpdates	授予返回与指定文件关联的更新文件的 Amazon S3 预签名 URL 的权限 JobId	读取			
ListClusterJobs	授予列出指定长度 JobListEntry 对象的权限	列表			
ListClusters	授予列出指定长度 ClusterListEntry 对象的权限	列表			
ListCompatibleImages	授予返回您 Amazon Web Services 账户 拥有且支持在 Snow 设备上使用的不同 EC2 亚马逊系统映像 (AMIs) 列表的权限	列表			
ListJobs	授予列出指定长度 JobListEntry 对象的权限	列表			
ListLongTermPricing	为提出请求的账户授予列出 LongTermPricingListEntry 对象的权限	读取			
ListPickupLocations	授予权限以列出指定长度且取货时间可用的 Address 对象	列表			
ListServiceVersions	授予权限以列出 Snow 设备上服务的所有受支持版本	列表			
UpdateCluster	授予更新权限，当集群的 ClusterState 值处于 AwaitingQuorum 状态时，你可以更新与集群关联的某些信息	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateJob	当任务的 JobState 值为 “新建” 时，授予更新权限，您可以更新与作业关联的某些信息	写入			
UpdateJobShipmentState	授予权限以在当发运状态变成其他状态时更新状态。	写入			
UpdateLongTermPricing	授予权限以更新作业的特定预付费合同	写入			

Amazon Snowball 定义的资源类型

Amazon Snowball 不支持在 IAM 策略声明的`Resource`元素中指定资源 ARN。要允许对 Amazon Snowball 的访问权限，请在策略中指定 `"Resource": "*"`。

Amazon Snowball 的条件键

Snowball 没有可以在策略语句的 `Condition` 元素中使用的服务特定上下文键。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon SNS 的操作、资源和条件键

Amazon SNS（服务前缀：`sns`）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon SNS 定义的操作

- Amazon SNS 定义的资源类型
- Amazon SNS 的条件键

Amazon SNS 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddPermission	授予向主题的访问控制策略添加语句的权限，授予指定 Amazon 账户对指定操作的访问权限	权限管理	topic*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CheckIfPhoneNumberIsOptedOut	接受电话号码并指明电话持有者是否已选择不接收来自您的账户的 SMS 消息。	Read			
ConfirmSubscription	在本示例中，您将通过更早的订阅操作验证发送到终端节点的令牌来验证终端节点所有者接收消息的意图。	Write	topic*		
CreatePlatformApplication	为设备和移动应用程序可能注册的受支持推送通知服务（如 &APNS; 和 &GCM;）之一创建平台应用程序对象。	Write			iam:PassRole
CreatePlatformEndpoint	为受支持推送通知服务（例如 GCM 和 APNS）之一上的设备和移动应用程序创建终端节点。	写入			
CreateSMSSandboxPhoneNumber	授予添加目标电话号码并向该电话号码发送一次性密码 (OTP) 的权限 Amazon Web Services 账户	写入			
CreateTopic	授予创建可向其发布通知的主题的权限	Write	topic*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteEndpoint	授予从 Amazon SNS 中删除设备和移动应用程序的终端节点的权限	Write			
DeletePlatformApplication	这可授予创建一个平台应用程序对象的权限，用于受支持的推送通知服务，如 &APNS; 和 &GCM;。	写入			
DeleteSMSSandboxPhoneNumber	授予删除已验证或待处理 Amazon Web Services 账户的电话号码的权限	写入			
DeleteTopic	授予删除主题及其所有订阅的权限	写入	topic*		
GetDataProtectionPolicy	授予返回主题数据保护策略的权限	读取	topic*		
GetEndpointAttributes	为受支持推送通知服务（GCM 和 APNS）之一上的设备检索终端节点属性。	Read			
GetPlatformApplicationAttributes	检索用于受支持推送通知服务（例如 APNS 和 GCM）的平台应用程序对象的属性。	Read			
GetSMSAttributes	授予从您的帐户返回发送 SMS 消息的设置的权限	Read			
GetSMSSandboxAccountStatus	授予检索目标区域中呼叫账户的沙箱状态的权限	Read			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetSubscriptionAttributes	授予返回订阅的所有属性的权限	Read			
GetTopicAttributes	授予返回主题所有属性的权限	Read	topic*		
ListEndpointsByPlatformApplication	列出受支持推送通知服务（例如 GCM 和 APNS）中的设备的终端节点和终端节点属性。	List			
ListOriginationNumbers	授予列出所有原始编号及其元数据的权限	List			
ListPhoneNumbersOptedOut	返回已退出电话号码的列表，这意味着您无法向这些电话号码发送 SMS 消息。	Read			
ListPlatformApplications	列出用于受支持推送通知服务（例如 APNS 和 GCM）的平台应用程序对象。	List			
ListSMSSandboxPhoneNumbers	授予列出呼叫账户当前待处理和已验证的目标电话号码的权限	List			
ListSubscriptions	授予返回请求者订阅列表的权限	List			
ListSubscriptionsByTopic	授予检索对特定主题的所有订阅的权限。	List	topic*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListTagsForResource	授予列出添加到指定 Amazon SNS 主题的所有标签的权限	Read	topic		
ListTopics	授予返回请求者主题列表的权限	List			
OptInPhoneNumber	加入当前已退出的电话号码，这样您便可以继续向该号码发送 SMS 消息。	Write			
Publish	授予向主题的所有订阅终端节点发送消息的权限	写入	topic*		
PutDataProtectionPolicy	授予允许主题所有者设置数据保护策略的权限	写入	topic*		
RemovePermission	授予从主题的访问控制策略中删除语句的权限	Permissions management	topic*		
SetEndpointAttributes	为受支持推送通知服务（GCM 和 APNS）之一上的设备设置终端节点属性。	Write			
SetPlatformApplicationAttributes	为用于受支持推送通知服务（例如 APNS 和 GCM）的平台应用程序对象设置属性。	Write			iam:PassRole
SetSMSAttributes	设置用于发送 SMS 消息和接收每日 SMS 使用情况报告的默认设置。	Write			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
SetSubscriptionAttributes	授予允许订阅所有者将主题属性设置为新值的权限	Write			
SetTopicAttributes	授予允许主题所有者将主题属性设置为新值的权限	权限管理	topic*		iam:PassRole
Subscribe	通过向终端节点发送确认消息，授予准备订阅终端节点的权限	Write	topic*		
				sns:Endpoint sns:Protocol	
TagResource	授予向指定的 Amazon SNS 主题添加标签的权限	Tagging	topic		
				aws:RequestTag/${TagKey} aws:TagKeys	
Unsubscribe	授予权限以删除订阅定义。	Write			
UntagResource	授予从 Amazon SNS 指定服务器或备份中删除标签的权限	标记	topic		
				aws:TagKeys	
VerifySMSSandboxPhoneNumber	授予使用一次性密码 (OTP) 验证目标电话号码的权限 Amazon Web Services 账户	写入			

Amazon SNS 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
topic	arn:${Partition}:sns:${Region}:${Account}:${TopicName}	aws:ResourceTag/${TagKey}

Amazon SNS 的条件键

Amazon SNS 定义以下可以在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中的标签键筛选访问权限	ArrayOfString
sns:Endpoint	按订阅请求或以前确认的订阅中的 URL、电子邮件地址或 ARN 筛选访问权限	字符串
sns:Protocol	按订阅请求或以前确认的订阅中的协议值筛选访问权限	字符串

Amazon SQL Workbench 的操作、资源和条件键

Amazon SQL Workbench（服务前缀:sqlworkbench）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

由 Amazon SQL Workbench 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateConnectionWithChart[仅权限]	授予将连接与图表关联的权限	写入	chart*		
			connection*		
AssociateConnectionWithTab[仅权限]	授予将连接与选项卡关联的权限	写入	connection*		
AssociateNotebookWithTab[仅权限]	授予将笔记本与选项卡关联的权限	写入	notebook*		
AssociateQueryWithTab[仅权限]	授予将查询与选项卡关联的权限	写入	query*		
BatchDeleteFolder[仅权限]	授予权限以删除账户上的文件夹	写入			
BatchGetNotebookCell[仅权限]	授予获取账户上笔记本单元格内容的权限	读取	notebook*		
CreateAccount[仅权限]	授予创建 SQLWorkbench 账户的权限	写入			
CreateChart[仅权限]	授予权限以在账户上创建新保存的图表	写入	chart*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateConnection[仅权限]	授予权限以在账户上创建新连接	写入	connection*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateFolder[仅权限]	授予权限以在账户上创建文件夹	写入			
CreateNotebook[仅权限]	授予在账户上创建新笔记本的权限	写入	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateNotebookCell[仅权限]	授予在账户上创建笔记本单元格的权限	写入	notebook*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateNotebookFromVersion[仅权限]	授予在账户上从笔记本版本创建新笔记本的权限	写入	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateNotebookVersion[仅权限]	授予在账户上创建笔记本版本的权限	写入	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateSavedQuery[仅权限]	授予权限以在账户上创建新保存的查询	写入	query*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteChart[仅权限]	授予权限以删除账户上的图表	写入	chart*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteConnection[仅权限]	授予权限以删除账户上的连接	写入	connection*		
DeleteNotebook[仅权限]	授予在账户上移除笔记本的权限	写入	notebook*		
DeleteNotebookCell[仅权限]	授予在账户上移除笔记本单元格的权限	写入	notebook*		
DeleteNotebookVersion[仅权限]	授予在账户上移除笔记本单元格的权限	写入	notebook*		
DeleteQCustomContext[仅权限]	授予权限以删除账户范围的自定义上下文	写入			
DeleteSavedQuery[仅权限]	授予权限以删除账户上已保存的查询	写入	query*		
DeleteSqlGenerationContext[仅权限]	授予删除 sql 生成上下文的权限	写入			
DeleteTab[仅权限]	授予权限以删除账户上的选项卡	写入			
DriverExecute[仅权限]	授予权限以在 Redshift 集群中执行查询	写入	connection*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DuplicateNotebook[仅权限]	授予在账户上通过复制现有笔记本来创建新笔记本的权限	写入	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ExportNotebook[仅权限]	授予在账户上导出笔记本的权限	读取	notebook*		
GenerateSession[仅权限]	授予权限以在账户上生成新会话	写入			
GetAccountInfo[仅权限]	授予权限以获取账户信息	读取			
GetAccountSettings[仅权限]	授予获取账户设置的权限	读取			
GetAutocompletionMetadata[仅权限]	授予权限以获取数据库结构元数据以实现自动完成	读取			
GetAutocompletionResource[仅权限]	授予权限以获取数据库结构信息以实现自动完成	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetChart[仅权限]	授予权限以获取账户上的图表	读取	chart*		
GetConnection[仅权限]	授予权限以获取账户上的连接	读取	connection*		
GetNotebook[仅权限]	授予在账户上获取笔记本元数据的权限	读取	notebook*		
GetNotebookVersion[仅权限]	授予在账户上获取笔记本版本内容的权限	读取	notebook*		
GetQCustomContext[仅权限]	授予权限以获取账户范围的自定义上下文	读取			
GetQSqlPromptQuotas[仅权限]	授予权限以获取 Q 生成式 SQL 最大提示配额	读取			
GetQSqlRecommendations[仅权限]	授予获取从文本转 SQL 建议的权限	读取			
GetQueryExecutionHistory[仅权限]	授予获取账户的查询执行历史记录的权限	读取			
GetSavedQuery[仅权限]	授予权限以获取账户上已保存的查询	读取	query*		
GetSchemaInference[仅权限]	授予权限以获取从文件推断的列和数据类型	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetSqlGenerationContext[仅权限]	授予获取 sql 生成上下文的权限	读取			
GetSqlRecommendations[仅权限]	授予获取从文本转 SQL 建议的权限	读取			
GetUserInfo[仅权限]	授予权限以获取用户信息	读取			
GetUserWorkspaceSettings[仅权限]	授予权限以获取账户中的工作区设置	读取			
ImportNotebook[仅权限]	授予在账户上导入笔记本的权限	写入	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ListConnections[仅权限]	授予权限以列出账户上的连接	列表			
ListDatabases[仅权限]	授予权限以列出 Redshift 集群的数据库	列表			
ListFiles[仅权限]	授予权限以列出文件和文件夹	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListNotebookVersions[仅权限]	授予在账户上获取笔记本版本元数据的权限	列表	notebook*		
ListNotebooks[仅权限]	授予在账户上列出笔记本的权限	列表			
ListQueryExecutionHistory[仅权限]	授予列出账户的查询执行历史记录的权限	列表			
ListRedshiftClusters[仅权限]	授予权限以列出账户上的 Redshift 集群	列表			
ListSampleDatabases[仅权限]	授予权限以列出示例数据库	读取			
ListSavedQueryVersions[仅权限]	授予权限以列出账户上已保存的查询的版本	列表	query*		
ListTabs[仅权限]	授予权限以列出账户中的选项卡	列表			
ListTaggedResources[仅权限]	授予列出标记的资源的权限	读取			
ListTagsForResource[仅权限]	授予权限以列出 sqlworkbench 资源的标签	读取	chart		
			connection		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			notebook		
			query		
PassAccountSettings[仅权限]	授予在请求中提供账户设置的权限	写入			
PutQCustomContext[仅权限]	授予权限以更新账户范围的自定义上下文	写入			
PutSqlGenerationContext[仅权限]	授予更新 sql 生成上下文的权限	写入			
PutTab[仅权限]	授予权限以创建或更新账户上的选项卡	写入			
PutUserWorkspaceSettings[仅权限]	授予权限以更新账户中的工作区设置	写入			
RestoreNotebookVersion[仅权限]	授予在账户上将笔记本恢复到某个版本的权限	写入	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagResource[仅权限]	授予权限以标记 sqlworkbench 资源	标记	chart		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			connection		
			notebook		
			query		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource[仅权限]	授予权限以取消标记 sqlworkbench 资源	标记	chart		
			connection		
			notebook		
			query		
				aws:TagKeys	
UpdateAccountConnectionSettings[仅权限]	授予权限以更新账户范围的连接设置	写入			
UpdateAccountExportSettings[仅权限]	授予权限以更新账户范围的导出设置	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateAccountGeneralSettings[仅权限]	授予权限以更新账户范围的常规设置	写入			
UpdateAccountQSqlSettings[仅权限]	授予更新账户范围的文本转 SQL 设置的权限	写入			
UpdateChart[仅权限]	授予权限以更新账户上的图表	写入	chart*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateConnection[仅权限]	授予权限以更新账户上的连接	写入	connection*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateFileFolder[仅权限]	授予权限以移动账户上的文件	写入	chart		
			query		
UpdateFolder[仅权限]	授予权限以更新账户上的文件夹名称和详细信息	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateNotebook[仅权限]	授予在账户上更新笔记本元数据的权限	写入	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateNotebookCellContent[仅权限]	授予在账户上更新笔记本单元格内容的权限	写入	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateNotebookCellLayout[仅权限]	授予在账户上更新笔记本单元格布局的权限	写入	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateSavedQuery[仅权限]	授予权限以更新账户上已保存的查询	写入	query*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Amazon SQL Workbench 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}

Amazon SQL Workbench 的条件键

Amazon SQL Workbench 定义了以下可以在 IAM 策略Condition元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串

条件键	描述	类型
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString

Amazon SQS 的操作、资源和条件键

Amazon SQS（服务前缀：sqs）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon SQS 定义的操作
- Amazon SQS 定义的资源类型
- Amazon SQS 的条件键

Amazon SQS 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddPermission	为特定委托人的队列授予权限	权限管理	queue*		
CancelMessageMoveTask	授予权限以取消正在进行的消息移动任务	写入	queue*		
ChangeMessageVisibility	授予权限以将队列中指定消息的可见性超时更改为新值	写入	queue*		
CreateQueue	授予权限以创建新的队列，或返回现有队列的 URL	写入	queue*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteMessage	授予权限以从指定队列中删除指定的消息	写入	queue*		
DeleteQueue	授予权限以删除由队列 URL 指定的队列，无论队列是否为空	写入	queue*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetQueueAttributes	授予权限以获取指定队列的属性	读取	queue*		
GetQueueUrl	授予权限以返回现有队列的 URL	读取	queue*		
ListDeadLetterSourceQueues	授予返回队列列表的权限，这些队 RedrivePolicy 列的队列属性配置了死信队列	读取	queue*		
ListMessageMoveTasks	授予权限以列出消息移动任务	读取	queue*		
ListQueueTags	授予权限以列出已添加到 SQS 队列的标签	读取	queue*		
ListQueues	授予权限以返回队列列表	读取			
PurgeQueue	授予权限以删除由队列 URL 指定的队列中的消息	写入	queue*		
ReceiveMessage	授予权限以从指定的队列检索一条或多条消息，最大限制为 10 条消息	读取	queue*		
RemovePermission	授予权限以撤销与指定的标签参数匹配的队列策略中的任何权限	权限管理	queue*		
SendMessage	授予权限以将消息传输到指定队列中	写入	queue*		
SetQueueAttributes	授予权限以设置一个或多个队列属性的值	写入	queue*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StartMessageMoveTask	授予权限以启动消息移动任务	写入	queue*		
TagQueue	授予权限以向指定的 SQS 队列添加标签	标记	queue*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagQueue	授予权限以从指定的 SQS 队列中删除标签	标记	queue*		
				aws:TagKeys	

Amazon SQS 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

> **Note**
>
> 队列的 ARN 仅在 IAM 权限策略中使用。在 API 和 CLI 调用中，您可以改用队列的 URL。

资源类型	ARN	条件键
queue	arn:${Partition}:sqs:${Region}:${Account}:${QueueName}	aws:ResourceTag/${TagKey}

Amazon SQS 的条件键

Amazon SQS 定义以下可以在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString

Amazon Step Functions 的操作、资源和条件键

Amazon Step Functions（服务前缀:states）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Step Functions 定义的操作
- Amazon Step Functions 定义的资源类型
- Amazon Step Functions 的条件键

Amazon Step Functions 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateActivity	授予创建活动的权限	Write	activity*		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateStateMachine	授予创建状态机的权限	写入	statemachine*		iam:PassRole states:PublishStateMachineVersion
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStateMachineAlias	授予创建状态机别名的权限	写入	statemachine*		
				states:StateMachineQualifier	
DeleteActivity	授予删除活动的权限	Write	activity*		
DeleteStateMachine	授予删除状态机的权限	写入	statemachine*		
DeleteStateMachineAlias	授予删除状态机别名的权限	写入	statemachine*		
				states:StateMachineQualifier	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteStateMachineVersion	授予删除状态机版本的权限	写入	statemachine*		
				states:StateMachineQualifier	
DescribeActivity	授予描述活动的权限	Read	activity*		
DescribeExecution	授予描述执行的权限	读取	execution*		
			express*		
DescribeMapRun	授予权限以描述映射运行	读取	maprun*		
DescribeStateMachine	授予描述状态机的权限	读取	statemachine*		
				states:StateMachineQualifier	
DescribeStateMachineAlias	授予描述状态机别名的权限	读取	statemachine*		
				states:StateMachineQualifier	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeStateMachineForExecution	授予描述执行状态机的权限	Read	execution*		
GetActivityTask	授予工作线程用于检索正在运行的状态机安排执行的任务（通过指定活动 ARN）的权限	Write	activity*		
GetExecutionHistory	授予将指定执行历史记录作为事件列表返回的权限	读取	execution*		
InvokeHTTPEndpoint[仅权限]	授予调用 HTTP Task 状态的权限	写入			
ListActivities	授予列出现有活动的权限	List			
ListExecutions	授予列出状态机执行的权限	列表	maprun*		
			statemachine*		
				states:StateMachineQualifier	
ListMapRuns	授予权限以列出执行的映射运行	列表	execution*		
ListStateMachineAliases	授予列出状态机别名的权限	列表	statemachine*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				states:StateMachineQualifier	
ListStateMachineVersions	授予列出状态机版本的权限	列表	statemachine*		
ListStateMachines	授予列出现有状态机的权限	列表			
ListTagsForResource	授予列出 Ste Amazon p Functions 资源标签的权限	列表	activity		
			statemachine		
PublishStateMachineVersion	授予发布状态机版本的权限	写入	statemachine*		
RedriveExecution	授予重新驱动执行的权限	写入	execution*		
RevealSecrets[仅权限]	授予检索执行中的敏感数据的权限	读取			
SendTaskFailure	授予工作线程用于报告由 taskToken 标识的任务已失败的权限	Write			
SendTaskHeartbeat	授予工作线程用于向服务报告，由指定的 taskToken 表示的任务仍在进行中的权限	Write			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
SendTaskSuccess	授予工作线程用于报告由 taskToken 标识的任务已成功完成的权限	Write			
StartExecution	授予启动状态机执行的权限	Write	statemachine*		
				states:StateMachineQualifier	
StartSyncExecution	授予启动 Synchronous Express 状态机执行的权限	Write	statemachine*		
				states:StateMachineQualifier	
StopExecution	授予停止执行的权限	写入	execution*		
TagResource	授予标记 Ste Amazon p Functions 资源的权限	标记	activity		
			statemachine		
				aws:TagKeys aws:RequestTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
TestState	授予测试状态机定义的权限	写入			states:RevealSecrets
UntagResource	授予从 Ste Amazon p Functions 资源中移除标签的权限	标记	activity		
			statemachine		
				aws:TagKeys	
UpdateMapRun	授予权限以更新映射运行	写入	maprun*		
UpdateStateMachine	授予更新状态机的权限	写入	statemachine*		iam:PassRole states:PublishStateMachineVersion
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateStateMachineAlias	授予更新状态机别名的权限	写入	statemachine*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				states:StateMachineQualifier	
ValidateStateMachineDefinition	授予权限以测试状态机定义	读取			

Amazon Step Functions 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}

资源类型	ARN	条件键
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}	

Amazon Step Functions 的条件键

Amazon Step Functions 定义了以下可以在 IAM 策略Condition元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中允许的标签键值对筛选访问	字符串
aws:ResourceTag/${TagKey}	按某个资源的标签键值对筛选访问	字符串

条件键	描述	类型
aws:TagKeys	按请求中允许的标签键列表筛选访问	ArrayOfString
states:HTTPEndpoint	按请求中的 HTTP Task 状态允许的端点筛选访问权限	字符串
states:HTTPMethod	按请求中的 HTTP Task 状态允许的方法筛选访问权限	字符串
states:StateMachineQualifier	按状态机 ARN 的限定符筛选访问权限	ArrayOfString

Amazon Storage Gateway 的操作、资源和条件键

Amazon Storage Gateway（服务前缀:`storagegateway`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- 由 Amazon Storage Gateway 定义的操作
- 由 Amazon Storage Gateway 定义的资源类型
- Amazon Storage Gateway 的条件键

由 Amazon Storage Gateway 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ActivateGateway	授予以下权限：激活您之前在主机上部署的网关	Write		aws:RequestTag/${TagKey} aws:TagKeys	
AddCache	授予以下权限：将一个或多个网关本地磁盘配置为缓存卷网关的缓存	Write	gateway*		
AddTagsToResource	授予将一个或多个标签添加到指定资源的权限	Tagging	cache-report		
			fs-association		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			gateway		
			share		
			tape		
			tapepool		
			volume		
				aws:RequestTag/${TagKey} aws:TagKeys	
AddUploadBuffer	授予以下权限：将一个或多个网关本地磁盘配置为指定网关的上传缓冲区	Write	gateway*		
AddWorkingStorage	授予以下权限：将一个或多个网关本地磁盘配置为网关的工作存储	Write	gateway*		
AssignTapePool	授予以下权限：将磁带移动到指定的目标池	写入	tape*		
			tapepool*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateFileSystem	授予将亚马逊 FSx 文件系统与亚马逊 FSx 文件网关关联的权限	写入	gateway*		ds:DescribeDirectories ec2:DescribeNetworkInterfaces fsx:DescribeFileSystems iam:CreateServiceLinkedRole logs:CreateLogDelivery logs:GetLogDelivery logs:ListLogDeliveries logs:UpdateLogDelivery

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
AttachVolume	授予以下权限：将卷连接到 iSCSI 连接，然后将卷附加到指定的网关	Write	gateway*		
			volume*		
BypassGovernanceRetention	授予以下权限：允许绕过池上的监管保留锁定	Write	tapepool*		
CancelArchival	授予权限：取消已经启动的将虚拟磁带存档到虚拟磁带架 (VTS) 的过程	写入	gateway*		
			tape*		
CancelCacheReport	授予取消缓存报告的权限	写入	cache-report*		
CancelRetrieval	授予以下权限：取消已经启动的从虚拟磁带架 (VTS) 到网关检索虚拟磁带的过程	Write	gateway*		
			tape*		
CreateCachediSCSIVolume	授予以下权限：在指定缓存网关上创建缓存卷 只有网关缓存卷架构才支持此操作	Write	gateway*		
			volume*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNFSFileShare	授予以下权限：在现有文件网关上创建 NFS 文件共享	Write	gateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSMBFileShare	授予以下权限：在现有文件网关上创建 SMB 文件共享	Write	gateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshot	授予以下权限：开始创建卷快照	Write	volume*		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateSnapshotFromVolumeRecoveryPoint	授予以下权限：从卷恢复点开始创建网关快照	Write	volume*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStorediSCSIVolume	授予以下权限：在指定网关上创建卷	Write	gateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTapePool	授予以下权限：创建磁带池	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTapeWithBarcode	授予以下权限：使用您自己的条形码创建虚拟磁带	Write	gateway*		
			tapepool*		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateTapes	授予以下权限：创建一个或多个虚拟磁带。您将数据写入虚拟磁带，然后将其存档	Write	gateway*		
			tapepool*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAutomaticTapeCreationPolicy	授予以下权限：删除在网关 VTL 上配置的自动磁带创建策略	Write	gateway*		
DeleteBandwidthRateLimit	授予以下权限：删除网关的带宽速率限制	写入	gateway*		
DeleteCacheReport	授予删除与缓存报告关联的元数据的权限	写入	cache-report*		
DeleteChapCredentials	授予以下权限：删除指定的 iSCSI 目标及其配套启动程序的质询握手身份验证协议 (CHAP) 凭证	Write	target*		
DeleteFileShare	授予以下权限：从文件网关删除文件共享	Write	share*		
DeleteGateway	授予权限以删除网关	Write	gateway*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteSnapshotSchedule	授予以下权限：删除卷快照	Write	volume*		
DeleteTape	授予以下权限：删除指定虚拟磁带	Write	gateway*		
			tape*		
DeleteTapeArchive	授予以下权限：从虚拟磁带架 (VTS) 中删除指定虚拟磁带	Write			
DeleteTapePool	授予以下权限：删除指定磁带池	写入	tapepool*		
DeleteVolume	授予删除您之前使用 CreateCachediSCSIVolume 或 CreateStoredi SCSIVolume API 创建的指定网关卷的权限	写入	volume*		
DescribeAvailabilityMonitorTest	授予以下权限：获取在网关上执行的最新高可用性监控测试的相关信息	Read	gateway*		
DescribeBandwidthRateLimit	授予以下权限：获取网关的带宽速率限制	Read	gateway*		
DescribeBandwidthRateLimitSchedule	授予以下权限：获取网关的带宽速率限制计划	Read	gateway*		
DescribeCache	授予以下权限：获取网关的缓存信息。只有网关缓存卷架构才支持此操作	读取	gateway*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeCacheReport	授予获取缓存报告描述的权限	读取	cache-report*		
DescribeCachediSCSIVolumes	授予以下权限：获取请求中指定网关卷的描述。只有网关缓存卷架构才支持此操作	Read	volume*		
DescribeChapCredentials	授予以下权限：获取指定 iSCSI 目标的质询握手身份验证协议 (CHAP) 凭证信息，每对“目标–启动程序”一个	Read	target*		
DescribeFileSystemAssociations	授予以下权限：获取一个或多个文件系统关联的描述	Read	fs-association*		
DescribeGatewayInformation	授予以下权限：获取有关网关的元数据，如名称、网络接口、已配置的时区和状态（网关运行与否）	Read	gateway*		
DescribeMaintenanceStartTime	授予以下权限：获取网关的周度维护起始时间信息，包括一星期中的天和时间	Read	gateway*		
DescribeNFSFileShares	授予以下权限：从文件网关获取一个或多个文件共享的描述	Read	share*		
DescribeSMBFileShares	授予以下权限：从文件网关获取一个或多个文件共享的描述	Read	share*		
DescribeSMBSettings	授予以下权限：从文件网关获取服务器消息块 (SMB) 文件共享设置的描述	Read	gateway*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeSnapshotSchedule	授予以下权限：描述指定网关卷的快照计划	Read	volume*		
DescribeStorediSCSIVolumes	授予以下权限：获取请求中指定网关卷的描述	Read	volume*		
DescribeTapeArchives	授予以下权限：获取虚拟磁带架 (VTS) 中指定虚拟磁带的描述	Read			
DescribeTapeRecoveryPoints	授予以下权限：获取指定网关 VTL 可用的虚拟磁带还原点的列表	Read	gateway*		
DescribeTapes	授予以下权限：获取虚拟磁带的指定 Amazon Resource Name (ARN) 的描述	Read	gateway*		
DescribeUploadBuffer	授予以下权限：获取网关的上传缓冲区的相关信息	Read	gateway*		
DescribeVTLDevices	授予以下权限：获取指定网关的虚拟磁带库 (VTL) 设备的描述	Read	gateway*		
DescribeWorkingStorage	授予以下权限：获取网关的工作存储的相关信息	Read	gateway*		
DetachVolume	授予以下权限：断开卷与 iSCSI 的连接，然后将卷从指定网关中分离	Write	volume*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DisableGateway	授予以下权限：在网关不再运行时禁用网关	写入	gateway*		
DisassociateFileSystem	授予解除亚马逊 FSx 文件系统与亚马逊文件网关关联的权限 FSx	写入	fs-association*		
EvictFilesFailingUpload	授予清除共享缓存中无法上传到 Amazon S3 的文件条目的权限	写入	share*		
JoinDomain	授予以下权限：允许您加入 Active Directory 域	写入	gateway*		
ListAutomaticTapeCreationPolicies	授予列出在指定网关 VTL 或您拥有的所有网关上配置的自动磁带创建策略的权限 VTLs Amazon Web Services 账户	列表			
ListCacheReports	授予获取您拥有的缓存报告列表的权限 Amazon Web Services 账户	列表			
ListFileShares	授予获取特定文件网关的文件共享列表或您拥有的文件共享列表的权限 Amazon Web Services 账户	列表			
ListFileSystemAssociations	授予以下权限：获取指定网关的文件系统关联列表	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListGateways	授予列出请求 Amazon Web Services 账户 中指定区域内由拥有的网关的权限。返回的列表按网关 Amazon Resource Name (ARN) 排序	List			
ListLocalDisks	授予以下权限：获取网关本地磁盘的列表	List	gateway*		
ListTagsForResource	授予以下权限：获取已添加到指定资源的标签	列表	gateway		
			share		
			tape		
			volume		
ListTapePools	授予列出您拥有的磁带池的权限 Amazon Web Services 账户	列表			
ListTapes	授予以下权限：列出您的虚拟磁带库 (VTL) 和虚拟磁带架 (VTS) 中的虚拟磁带	List			
ListVolumeInitiators	授予以下权限：列出与卷连接的 iSCSI 启动程序	List	volume*		
ListVolumeRecoveryPoints	授予以下权限：列出指定网关的恢复点	List	gateway*		
ListVolumes	授予以下权限：列出网关的 iSCSI 存储卷	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
NotifyWhenUploaded	当写入您的 NFS 文件共享的所有文件都已上传到 Amazon S3 时，授予通过 CloudWatch 事件向您发送通知的权限	写入	share*		
RefreshCache	授予以下权限：刷新指定文件共享的缓存	Write	share*		
RemoveTagsFromResource	授予从指定资源中删除一个或多个标签的权限	Tagging	cache-report		
			fs-association		
			gateway		
			share		
			tape		
			tapepool		
			volume		
				aws:TagKeys	
ResetCache	授予以下权限：重置所有遇到错误的缓存磁盘，并将它们设为可用状态，以便重新配置为缓存存储	Write	gateway*		
RetrieveTapeArchive	授予以下权限：检索从虚拟磁带架 (VTS) 存档到网关 VTL 的虚拟磁带	Write	gateway*		
			tape*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
RetrieveTapeRecoveryPoint	授予以下权限：检索指定虚拟磁带的恢复点	Write	gateway*		
			tape*		
SetLocalConsolePassword	授予以下权限：为 VM 本地控制台设置密码	Write	gateway*		
SetSMBGuestPassword	授予以下权限：为 SMB Guest 用户设置密码	Write	gateway*		
ShutdownGateway	授予以下权限：关闭网关	Write	gateway*		
StartAvailabilityMonitorTest	授予以下权限：启动测试，以验证是否已为主机环境中的高可用性监控配置指定网关	写入	gateway*		
StartCacheReport	授予启动现有文件共享缓存报告的权限	写入	share*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartGateway	授予以下权限：启动您之前关闭的网关	Write	gateway*		
UpdateAutomaticTapeCreationPolicy	授予以下权限：更新网关 VTL 上配置的自动磁带创建策略	Write	gateway*		
			tapepool*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateBandwidthRateLimit	授予以下权限：更新网关的带宽速率限制	Write	gateway*		
UpdateBandwidthRateLimitSchedule	授予以下权限：更新网关的带宽速率限制计划	Write	gateway*		
UpdateChapCredentials	授予以下权限：更新指定 iSCSI 目标的质询握手身份验证协议 (CHAP) 凭证	Write	target*		
UpdateFileSystemAssociation	授予以下权限：更新文件系统关联	Write	fs-association*		logs:CreateLogDelivery logs:DeleteLogDelivery logs:GetLogDelivery logs:ListLogDeliveries logs:UpdateLogDelivery

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateGatewayInformation	授予以下权限：更新网关的元数据，其中包括网关的名称和时区	Write	gateway*		
UpdateGatewaySoftwareNow	授予以下权限：更新网关虚拟机 (VM) 软件	Write	gateway*		
UpdateMaintenanceStartTime	授予以下权限：更新网关的周度维护起始时间信息，包括一星期中的天和时间。维护时间与网关时区中的时间一致	Write	gateway*		
UpdateNFSFileShare	授予以下权限：更新 NFS 文件共享	Write	share*		
UpdateSMBFileShare	授予以下权限：更新 SMB 文件共享	Write	share*		
UpdateSMBFileShareVisibility	授予以下权限：更新网关上的共享是以网络视图显示，还是以浏览列表显示	写入	gateway*		
UpdateSMBLocalGroups	授予更新对网关上的 SMB 文件共享具有特殊权限的 Active Directory 用户和组列表的权限	写入	gateway*		
UpdateSMBSecurityStrategy	授予以下权限：更新文件网关上的 SMB 安全策略	Write	gateway*		
UpdateSnapshotSchedule	授予以下权限：更新针对网关卷配置的快照计划	Write	volume*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateVTLDeviceType	授予以下权限：更新网关 VTL 中介质更换器的类型	写入	device*		

由 Amazon Storage Gateway 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}

资源类型	ARN	条件键
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}

Amazon Storage Gateway 的条件键

Amazon Storage Gateway 定义了以下可以在 IAM 策略Condition元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按每个标签的允许值集筛选访问	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签值筛选访问权限	字符串

条件键	描述	类型
aws:TagKeys	按请求中是否具有必需标签来筛选访问	ArrayOfString

Amazon Web Services 支持的操作、资源和条件键

Amazon Web Services 支持 （服务前缀:support）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Web Services 支持定义的操作
- Amazon Web Services 支持定义的资源类型
- Amazon Web Services 支持的条件键

Amazon Web Services 支持定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

> **Note**
>
> Amazon Web Services 支持 提供了访问、修改和解决案例以及使用 Trusted Advisor 操作的功能。当您使用 Support API 调用 Trusted Advisor 相关操作时，任何“trustedadvisor:*”操作都不会限制您的访问。“trustedadvisor:*”操作仅适用于 Amazon Web Services Management Console中的 Trusted Advisor。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddAttachmentsToSet	授予向 Amazon Web Services 支持 案例添加一个或多个附件的权限	写入			
AddCommunicationToCase	授予在 Amazon Web Services 支持 案例中添加客户通信的权限	写入			
CreateCase	授予创建新 Amazon Web Services 支持 案例的权限	写入			
DescribeAttachment	授予描述附件详细信息的权限	读取			
DescribeCaseAttributes	授予允许辅助服务读取 Amazon Web Services 支持 案	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
	例属性的权限。这是一项内部管理的功能				
DescribeCases	授予列出与给定输入相匹配的 Amazon Web Services 支持 案例的权限	读取			
DescribeCommunication	授予获取单个 Amazon Web Services 支持 案例的单一通信和附件的权限	读取			
DescribeCommunications	授予列出一个或多个 Amazon Web Services 支持 案例的通信和附件的权限	读取			
DescribeCreateCaseOptions	授予描述创建支持案例的可用选项的权限	读取			
DescribeIssueTypes	授予返回 Amazon Web Services 支持 案例问题类型的权限	读取			
DescribeServices	授予列出适用于每项 Amazon 服务的服务和类别的权限	读取			
DescribeSeverityLevels	授予列出可分配给 Amazon Web Services 支持 案例的严重性级别的权限	读取			
DescribeSupportLevel	授予返回 Amazon 账户标识符支持级别的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeSupportedLanguages	授予描述给定类别代码、服务代码和问题类型的可用支持语言的权限	读取			
DescribeTrustedAdvisorCheckRefreshStatuses	授予获取基于检查标识符列表的 Trusted Advisor 刷新检查状态的权限	读取			
DescribeTrustedAdvisorCheckResult	授予获取具有指定检查标识符的 Trusted Advisor 检查结果的权限	读取			
DescribeTrustedAdvisorCheckSummaries	授予获取具有指定检查标识符的 Trusted Advisor 检查结果摘要的权限	读取			
DescribeTrustedAdvisorChecks	授予获取所有可用的 Trusted Advisor 检查列表（包括名称、标识符、类别和描述）的权限	读取			
GetInteraction	授予权限以检索针对特定交互的账户和技术问题提供的个性化疑难解答帮助	读取			
InitiateCallForCase	授予在 Cent Amazon Web Services 支持 er 上发起呼叫的权限。这是一项内部托管功能	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
InitiateChatForCase	授予在 Amazon Web Services 支持 Center 上发起聊天的权限。这是一项内部管理的功能	写入			
PutCaseAttributes	授予允许次要服务将属性附加到 Amazon Web Services 支持 案例的权限。这是一项内部托管功能	写入			
RateCaseCommunication	授予对 Amazon Web Services 支持 案例沟通进行评分的权限	写入			
RefreshTrustedAdvisorCheck	授予请求刷新具有指定检查标识符的 Trusted Advisor 检查的权限	写入			
ResolveCase	授予解决 Amazon Web Services 支持 案例的权限	写入			
SearchForCases	授予返回与给定输入相匹配的 Amazon Web Services 支持 案例列表的权限	读取			
StartInteraction	授予启动特定互动的权限，以获得针对账户和技术问题的个性化疑难解答帮助	写入			

Amazon Web Services 支持定义的资源类型

Amazon Web Services 支持 不支持在 IAM 策略声明的`Resource`元素中指定资源 ARN。要允许对 Amazon Web Services 支持的访问权限，请在策略中指定 `"Resource": "*"`。

Amazon Web Services 支持的条件键

Support 没有可在策略语句的 Condition 元素中使用的服务特定上下文键。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon Systems Manager 的操作、资源和条件键

Amazon Systems Manager（服务前缀:ssm）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

Amazon Systems Manager 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AddTagsToResource	授予为指定 Amazon 资源添加或覆盖一个或多个标签的权限	标记	association		
			automation-execution		
			document		
			instance		
			maintenancewindow		
			managed-instance		
			opsitem		
			opsmetadata		
			parameter		
			patchbaseline		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			task		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
AssociateOpsItemRelatedItem	授予与关联 RelatedItem 的权限 OpsItem	写入	opsitem*		
CancelCommand	授予权限以取消指定的 Run Command 命令	Write			
CancelMaintenanceWindowExecution	授予权限以取消进行中的维护时段执行	写入	maintenancewindow*		
CreateActivation	授予创建激活的权限，该激活用于向 Systems Manager 注册本地服务器和虚拟机 (VMs)	写入		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssociation	授予权限以将指定的 Systems Manager 文档与指定的实例或其他目标关联	写入	association*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			document*		
			instance		
			managed-instance		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssociationBatch	授予在单个命令中合并多个 CreateAssociation 操作条目的权限	写入	document*		
			instance		
			managed-instance		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateDocument	授予权限以创建 Systems Manager SSM 文档	Write	document*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMaintenanceWindow	授予权限以创建维护时段	写入		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOpsItem	授予 OpsItem 在中创建的权限 OpsCenter	写入		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOpsMetadata	授予为 Amazon 资源创建 OpsMetadata 对象的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreatePatchBaseline	授予权限以创建修补程序基准	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateResourceDataSync	授予权限以创建资源数据同步配置，该配置定期从托管实例收集清单数据并更新 Amazon S3 存储桶中的数据	Write	resourcedatasync*		
				ssm:SyncType	
DeleteActivation	授予权限以删除托管实例的指定激活	Write			
DeleteAssociation	授予权限以从指定实例解除与指定 SSM 文档的关联	Write	association		
			document		
			instance		
			managed-instance		
				aws:ResourceTag/${TagKey}	
DeleteDocument	授予权限以删除指定 SSM 文档及其实例关联	Write	document*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteInventory	授予权限以删除指定的自定义清单类型或者与自定义清单类型关联的数据	Write			
DeleteMaintenanceWindow	授予权限以删除指定的维护时段	写入	maintenancewindow*		
DeleteOpsItem	授予删除的权限 OpsItem	写入	opsitem*		
DeleteOpsMetadata	授予删除 OpsMetadata 对象的权限	写入	opsmetadata*		
DeleteParameter	授予权限以删除一个指定的 SSM 参数	Write	parameter*		
				aws:ResourceTag/${TagKey}	
DeleteParameters	授予权限以删除多个指定的 SSM 参数	Write	parameter*		
				aws:ResourceTag/${TagKey}	
DeletePatchBaseline	授予权限以删除指定的补丁基准	Write	patchbaseline*		
DeleteResourceDataSync	授予权限以删除指定的资源数据同步	写入	resourcedatasync*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				ssm:SyncType	
DeleteResourcePolicy	授予删除 Systems Manager 资源策略的权限	权限管理	opsitemgroup		
			parameter		
DeregisterManagedInstance	授予权限以从 Systems Manager 取消注册指定的本地服务器或虚拟机 (VM)	Write	managed-instance*		
				ssm:resourceTag/tag-key	
DeregisterPatchBaselineForPatchGroup	授予权限以便为指定的补丁组取消注册作为默认补丁基准的指定补丁基准	Write	patchbaseline*		
DeregisterTargetFromMaintenanceWindow	授予权限以从维护时段取消注册指定的目标	Write	maintenancewindow*		
			windowtarget*		
DeregisterTaskFromMaintenanceWindow	授予权限以从维护时段取消注册指定的任务	Write	maintenancewindow*		
			windowtask*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeActivations	授予权限以查看有关指定托管实例激活的详细信息，例如其创建时间和使用激活注册的实例数	Read			
DescribeAssociation	授予权限以查看指定实例或目标的指定关联的相关详细信息	Read	association		
			document		
			instance		
			managed-instance		
				aws:ResourceTag/${TagKey}	
DescribeAssociationExecutionTargets	授予权限以查看有关指定关联执行情况的信息	Read	association*		
				aws:ResourceTag/${TagKey}	
DescribeAssociationExecutions	授予权限以查看指定关联的所有执行	Read	association*		
				aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeAutomationExecutions	授予权限以查看所有活动和已终止的 Automation 执行的相关详细信息	Read			
DescribeAutomationStepExecutions	授予权限以查看 Automation 工作流程中所有活动和已终止的步骤执行信息	Read	automation-execution*		
DescribeAvailablePatches	授予权限以查看符合包含在补丁基准中的条件的所有补丁	Read			
DescribeDocument	授予权限以查看有关指定 SSM 文档的详细信息	Read	document*		
DescribeDocumentParameters	授予权限以在 Systems Manager 控制台中显示有关 SSM 文档参数的信息（内部 Systems Manager 操作）	Read	document*		
DescribeDocumentPermission	授予权限以查看指定 SSM 文档的权限	Read	document*		
DescribeEffectiveInstanceAssociations	授予权限以查看指定实例的所有当前关联	Read	instance*		
			managed-instance*		
				aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeEffectivePatchesForPatchBaseline	授予权限以查看当前与指定补丁基准关联的补丁的相关详细信息（仅 Windows）	Read	patchbaseline*		
DescribeInstanceAssociationsStatus	授予权限以查看指定实例的关联的状态	Read	instance*		
			managed-instance*		
				aws:ResourceTag/${TagKey}	
DescribeInstanceInformation	授予权限以查看有关指定实例的详细信息	Read			
DescribeInstancePatchStates	授予权限以查看指定实例上有关补丁的状态详细信息	Read	instance*		
			managed-instance*		
				aws:ResourceTag/${TagKey}	
				ssm:resourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeInstancePatchStatesForPatchGroup	授予权限以描述指定修补程序组中实例的高级修补程序状态	Read			
DescribeInstancePatches	授予权限以查看有关指定实例上补丁的一般详细信息	读取	instance*		
			managed-instance*		
				aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}	
DescribeInstanceProperties	向用户的 Amazon EC2 控制台授予呈现托管实例节点的权限	读取			
DescribeInventoryDeletions	授予权限以查看有关指定库存删除的详细信息	Read			
DescribeMaintenanceWindowExecutionTaskInvocations	授予权限以查看某个维护时段的指定任务执行的详细信息	List			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeMaintenanceWindowExecutionTasks	授予权限以查看在指定维护时段执行期间运行的任务的相关详细信息	List			
DescribeMaintenanceWindowExecutions	授予权限以查看指定维护时段的执行	List	maintenancewindow*		
DescribeMaintenanceWindowSchedule	授予权限以查看有关指定维护时段即将开始的执行的详细信息	List			
DescribeMaintenanceWindowTargets	授予权限以查看与指定维护时段关联的目标的列表	List	maintenancewindow*		
DescribeMaintenanceWindowTasks	授予权限以查看与指定维护时段关联的任务的列表	List	maintenancewindow*		
DescribeMaintenanceWindows	授予权限以查看有关所有维护时段或指定维护时段的信息	List			
DescribeMaintenanceWindowsForTarget	授予权限以查看与指定实例关联的维护时段目标和任务相关的信息	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeOpsItems	授予权限以查看有关指定内容的详细信息 OpsItems	读取			
DescribeParameters	授予权限以查看有关指定 SSM 参数的详细信息	List			
DescribePatchBaselines	授予权限以查看符合指定条件的补丁基准的信息	List			
DescribePatchGroupState	授予权限以查看指定补丁组的补丁的聚合状态详细信息	列表			
DescribePatchGroups	授予权限以查看指定补丁组的补丁基准相关信息	List			
DescribePatchProperties	授予权限以查看指定操作系统和补丁属性的可用补丁的详细信息	List			
DescribeSessions	授予权限以查看满足指定搜索条件的近期会话管理器会话的列表	列表			
DisassociateOpsItemRelatedItem	授予取消关联 RelatedItem 的权限 OpsItem	写入	opsitem*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ExecuteAPI	向 Systems Manager 委派的管理员授予权限，使其能够查看中 OpsItems 多个 Amazon 账户的相关资源详细信息 Amazon Web Services Management Console	读取			
GetAutomationExecution	授予权限以查看指定 Automation 执行的详细信息	读取	automation-execution*		
				aws:ResourceTag/${TagKey}	
GetCalendar[仅权限]	授予查看特定日历详细信息的权限	读取	document*		
GetCalendarState	授予权限以查看更改日历或更改日历列表的日历状态	Read	document*		
GetCommandInvocation	授予权限以查看有关指定调用或插件的命令执行的详细信息	Read			
GetConnectionStatus	授予权限以查看指定托管实例的会话管理器连接状态	Read	instance		
			managed-instance		
			task		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				ssm:resourceTag/${TagKey} aws:ResourceTag/${TagKey}	
GetDefaultPatchBaseline	授予权限以查看指定操作系统类型的当前默认补丁基准	Read	patchbaseline*		
GetDeployablePatchSnapshotForInstance	授予权限以检索指定实例的当前补丁基准快照	Read			
GetDocument	授予权限以查看指定 SSM 文档的内容	读取	document*		
				ssm:DocumentCategories	
GetExecutionPreview	授予检索现有预览的权限，该预览显示了运行指定自动化 Runbook 会对目标资源产生的影响	读取			
GetInventory	授予权限以根据指定条件查看实例清单详细信息	Read			
GetInventorySchema	授予权限以查看指定清单项目类型的清单类型或属性名称的列表	Read			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetMaintenanceWindow	授予权限以查看有关指定维护时段的详细信息	Read	maintenancewindow*		
GetMaintenanceWindowExecution	授予权限以查看有关指定维护时段执行的详细信息	Read			
GetMaintenanceWindowExecutionTask	授予权限以查看有关指定维护时段执行任务的详细信息	Read			
GetMaintenanceWindowExecutionTaskInvocation	授予权限以查看在特定目标上运行的特定维护时段任务的详细信息	Read			
GetMaintenanceWindowTask	授予权限以查看在指定维护时段中注册的任务的详细信息	读取	maintenancewindow*		
GetManifest[仅权限]	为 Systems Manager 和 SSM Agent 授予权限以确定实例的包安装要求（内部 Systems Manager 调用）	读取			
GetOpsItem	授予查看有关指定信息的权限 OpsItem	读取	opsitem*		
GetOpsMetadata	授予检索 OpsMetadata 对象的权限	读取	opsmetadata*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetOpsSummary	OpsItems 根据指定的筛选器和聚合器授予查看有关摘要信息的权限	读取	resourcedatasync*		
GetParameter	授予权限以查看有关指定参数的信息	Read	parameter*		
				aws:ResourceTag/${TagKey}	
GetParameterHistory	授予权限以查看指定参数的详细信息和更改	Read	parameter*		
				aws:ResourceTag/${TagKey}	
GetParameters	授予权限以查看有关多个指定参数的信息	Read	parameter*		
				aws:ResourceTag/${TagKey}	
GetParametersByPath	授予权限以查看指定层次结构中参数的信息	Read	parameter*		
				ssm:Recursive	
GetPatchBaseline	授予权限以查看有关指定补丁基准的信息	Read	patchbaseline*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetPatchBaselineForPatchGroup	授予权限以查看指定补丁组的当前补丁基准的 ID	读取			
GetResourcePolicies	授予检索 Systems Manager 资源策略列表的权限	列表	opsitemgroup		
			parameter		
GetServiceSetting	授予查看服务的账户级别设置的权限 Amazon	读取	servicesetting*		
LabelParameterVersion	授予权限以将标识标签应用于参数的指定版本	Write	parameter*		
				aws:ResourceTag/${TagKey}	
ListAssociationVersions	授予权限以列出指定关联的版本	List	association*		
				aws:ResourceTag/${TagKey}	
ListAssociations	授予权限以列出指定 SSM 文档或托管实例的关联	List			
ListCommandInvocations	授予权限以列出有关发送到指定实例的命令调用的信息	列表			
ListCommands	授予权限以列出发送到指定实例的命令	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListComplianceItems	授予权限以列出指定资源上指定资源类型的合规性状态	List			
ListComplianceSummaries	授予权限以列出对于指定的合规性类型，合规以及不合规资源的摘要计数	List			
ListDocumentMetadataHistory	授予查看有关指定 SSM 文档的元数据历史记录的权限	列表	document*		
ListDocumentVersions	授予权限以列出指定文档的所有版本	List	document*		
ListDocuments	授予权限以查看指定 SSM 文档的相关信息	列表			
ListInstanceAssociations	授予 SSM Agent 检查新的 State Manager 关联（内部 Systems Manager 调用）的权限	列表	instance		
			managed-instance		
				aws:ResourceTag/${TagKey}	
ListInventoryEntries	授予权限以查看指定实例的指定清单类型的列表	列表			
ListNodes	授予基于指定筛选器查看托管节点详细信息的权限	列表	resourcedatasync*		
ListNodesSummary	授予基于指定筛选器和聚合器查看托管节点摘要信息的权限	列表	resourcedatasync*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListOpsItemEvents	授予查看相关详细信息的权限 OpsItemEvents	列表			
ListOpsItemRelatedItems	授予查看相关详细信息的权限 OpsItem RelatedItems	列表			
ListOpsMetadata	授予查看 OpsMetadata 对象列表的权限	列表			
ListResourceComplianceSummaries	授予权限以列出资源级摘要计数	List			
ListResourceDataSync	授予权限以列出有关账户中资源数据同步配置的信息	List		ssm:SyncType	
ListTagsForResource	授予权限以查看指定资源的资源标签的列表	列表	association		
			automation-execution		
			document		
			maintenancewindow		
			managed-instance		
			opsitem		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			opsmetadata		
			parameter		
			patchbaseline		
				aws:ResourceTag/${TagKey}	
ModifyDocumentPermission	授予与指定 Amazon 账户公开或私下共享自定义 SSM 文档的权限	权限管理	document*		
PutCalendar[仅权限]	授予创建/编辑特定日历的权限	写入	document*		
PutComplianceItems	授予权限以在指定资源上注册合规性类型和其他合规性详细信息	写入	instance		
			managed-instance		
				ssm:SourceInstanceARN ec2:SourceInstanceARN	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutConfigurePackageResult[仅权限]	为 SSM Agent 授予权限以生成特定代理请求结果的报告（内部 Systems Manager 调用）	读取			
PutInventory	授予权限以在多个指定的托管实例上添加或更新清单项目	Write			
PutParameter	授予权限以创建 SSM 参数	写入	parameter*		
				aws:RequestTag/${TagKey} aws:TagKeys ssm:Overwrite ssm:Policies	
PutResourcePolicy	授予创建或更新 Systems Manager 资源策略的权限	权限管理	opsitemgroup		
			parameter		
RegisterDefaultPatchBaseline	授予权限以便为操作系统类型指定默认补丁基准	写入	patchbaseline*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
RegisterManagedInstance	授予注册 Systems Manager Agent 的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	
RegisterPatchBaselineForPatchGroup	授予权限以便为指定的补丁组指定默认补丁基准	Write	patchbaseline*		
RegisterTargetWithMaintenanceWindow	授予权限以将目标注册到指定的维护时段	Write	maintenancewindow*		
RegisterTaskWithMaintenanceWindow	授予权限以将任务注册到指定的维护时段	Write	maintenancewindow*		
RemoveTagsFromResource	授予权限以从指定资源中删除指定标签键	标记	association		
			automation-execution		
			document		
			instance		
			maintenancewindow		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			managed-instance		
			opsitem		
			opsmetadata		
			parameter		
			patchbaseline		
			task		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ResetServiceSetting	授予将的服务设置重置 Amazon Web Services 账户 为默认值的权限	写入	servicesetting*		
ResumeSession	授予权限以将会话管理器会话重新连接到托管实例	Write	session*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				ssm:resourceTag/aws:ssmmessages:session-id ssm:resourceTag/aws:ssmmessages:target-id	
SendAutomationSignal	授予权限以发送信号，更改指定 Automation 执行的当前行为或状态	Write	automation-execution*		
				aws:ResourceTag/${TagKey}	
SendCommand	授予权限以在一个或多个指定托管实例上运行命令	Write	document*		
			bucket		
			instance		
			managed-instance		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}	
StartAssociationsOnce	授予权限以手动运行指定关联	Write	association*		
				aws:ResourceTag/${TagKey}	
StartAutomationExecution	授予权限以启动 Automation 文档的执行	Write	automation-definition*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartChangeRequestExecution	授予启动 Automation Change Template 文档的执行的权限	写入	automation-definition*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys ssm:AutoApprove	
StartExecutionPreview	授予创建预览的权限，该预览会显示运行指定的自动化运行手册会对目标资源产生的影响	读取			
StartSession	授予权限以便为会话管理器会话启动与指定目标的连接	Write	document		
			instance		
			managed-instance		
			task		
				ssm:resourceTag/${TagKey} aws:ResourceTag/${TagKey}	
StopAutomationExecution	授予权限以停止已在进行的指定 Automation 执行	Write	automation-execution*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey}	
TerminateSession	授予权限以永久结束与实例的会话管理器连接	写入	session*		
				ssm:resourceTag/aws:ssmmessages:session-id ssm:resourceTag/aws:ssmmessages:target-id	
UnlabelParameterVersion	授予从参数的指定版本移除标识标签的权限	写入	parameter*		
				aws:ResourceTag/${TagKey}	
UpdateAssociation	授予权限以更新关联并立即在指定目标上运行关联	Write	association*		
			document		
			instance		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			managed-instance		
				aws:ResourceTag/${TagKey}	
UpdateAssociationStatus	授予权限以更新与指定实例关联的 SSM 文档的状态	Write	document*		
			instance		
			managed-instance		
				ssm:SourceInstanceARN ec2:SourceInstanceARN aws:ResourceTag/${TagKey}	
UpdateDocument	授予权限以更新 SSM 文档的一个或多个值	Write	document*		
UpdateDocumentDefaultVersion	授予权限以更改 SSM 文档的默认版本	Write	document*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateDocumentMetadata	授予更新 SSM 文档元数据的权限	写入	document*		
UpdateInstanceAssociationStatus[仅权限]	为 SSM Agent 授予权限以更新当前正在运行的关联的状态（内部 Systems Manager 调用）	写入	association*		
			instance		
			managed-instance		
				ssm:SourceInstanceARN ec2:SourceInstanceARN aws:ResourceTag/${TagKey}	
UpdateInstanceInformation	为 SSM Agent 授予权限以向云中的 Systems Manager 服务发送检测信号	写入	instance		
			managed-instance		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				ssm:SourceInstanceARN ec2:SourceInstanceARN	
UpdateMaintenanceWindow	授予权限以更新指定的维护时段	Write	maintenancewindow*		
UpdateMaintenanceWindowTarget	授予权限以更新指定的维护时段目标	Write	maintenancewindow*		
			windowtarget*		
UpdateMaintenanceWindowTask	授予权限以更新指定的维护时段任务	Write	maintenancewindow*		
			windowtask*		
UpdateManagedInstanceRole	授予权限以分配或更改分配给指定托管实例的 IAM 角色	写入	iam-role*		
			managed-instance*		
				ssm:resourceTag/tag-key	
UpdateOpsItem	授予编辑或更改的权限 OpsItem	写入	opsitem*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateOpsMetadata	授予更新 OpsMetadata 对象的权限	写入	opsmetadata*		
UpdatePatchBaseline	授予权限以更新指定的补丁基准	Write	patchbaseline*		
UpdateResourceDataSync	授予权限以更新资源数据同步	写入	resourcedatasync*		
				ssm:SyncType	
UpdateServiceSetting	授予更新服务设置的权限 Amazon Web Services 账户	写入	servicesetting*		

Amazon Systems Manager 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

> **Note**
>
> 某些 State Manager API 参数已被弃用。这可能会导致意外行为。有关更多信息，请参阅使用 IAM 处理关联。

资源类型	ARN	条件键
association	arn:${Partition}:ssm:${Region}:${Account}:association/${AssociationId}	aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
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/${TagKey} ssm:DocumentCategories ssm:resourceTag/${TagKey}
iam-role	arn:${Partition}:iam::${Account}:role/${RoleName}	
instance	arn:${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

资源类型	ARN	条件键
managed-instance	arn:${Partition}:ssm:${Region}:${Account}:managed-instance/${InstanceId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
managed-instance-inventory	arn:${Partition}:ssm:${Region}:${Account}:managed-instance-inventory/${InstanceId}	
opsitem	arn:${Partition}:ssm:${Region}:${Account}:opsitem/${ResourceId}	aws:ResourceTag/${TagKey}
opsitemgroup	arn:${Partition}:ssm:${Region}:${Account}:opsitemgroup/default	
opsmetadata	arn:${Partition}:ssm:${Region}:${Account}:opsmetadata/${ResourceId}	aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}
parameter	arn:${Partition}:ssm:${Region}:${Account}:parameter/${ParameterNameWithoutLeadingSlash}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
patchbaseline	arn:${Partition}:ssm:${Region}:${Account}:patchbaseline/${PatchBaselineIdResourceId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key

资源类型	ARN	条件键
session	arn:${Partition}:ssm:${Region}:${Account}:session/${SessionId}	ssm:resourceTag/aws:ssmmessages:session-id ssm:resourceTag/aws:ssmmessages:target-id
resourcedatasync	arn:${Partition}:ssm:${Region}:${Account}:resource-data-sync/${SyncName}	
servicesetting	arn:${Partition}:ssm:${Region}:${Account}:servicesetting/${ResourceId}	
windowtarget	arn:${Partition}:ssm:${Region}:${Account}:windowtarget/${WindowTargetId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
windowtask	arn:${Partition}:ssm:${Region}:${Account}:windowtask/${WindowTaskId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
task	arn:${Partition}:ecs:${Region}:${Account}:task/${TaskId}	aws:ResourceTag/${TagKey}

Amazon Systems Manager 的条件键

Amazon Systems Manager 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据指定标签的允许值集按“创建”请求筛选访问权限	字符串
aws:ResourceTag/${TagKey}	根据分配给资源的标签键值对筛选访问权限 Amazon	字符串
aws:TagKeys	根据请求中是否具有必需标签按“创建”请求筛选访问权限	ArrayOfString
ec2:SourceInstanceARN	按发起请求的实例的 ARN 筛选访问	ARN
ssm:AutoApprove	通过验证用户是否有权启动 Change Manager 工作流而不执行某个审核步骤（变更冻结事件除外）来筛选访问权限	布尔型
ssm:DocumentCategories	通过验证用户是否有权访问属于特定类别的文档来筛选访问权限	ArrayOfString
ssm:Overwrite	按控制是否可以覆盖 Systems Manager 参数筛选访问权限	字符串
ssm:Policies	通过控制 IAM 实体（用户或角色）是否可以创建或更新包含参数策略的参数来筛选访问权限	字符串
ssm:Recursive	按在某个层次结构中创建的 Systems Manager 参数筛选访问权限	字符串
ssm:SourceInstanceARN	通过验证发出请求的 Amazon 系统管理员托管实例的 Amazon 资源名称 (ARN) 来筛选访问权限。当请求来自通过与实例配置文件关联的 IAM 角色进行身份验证的托管实例时，此密钥不存在 EC2	ARN
ssm:SyncType	通过验证用户是否也可以访问请求中 ResourceDataSync SyncType 指定的内容来筛选访问权限	字符串
ssm:resourceTag/${TagKey}	按分配给 Systems Manager 资源的标签键值对筛选访问权限	字符串

条件键	描述	类型
ssm:resourceTag/aws:ssmmessages:session-id	根据分配给 Systems Manager 会话资源的标签键/值对筛选访问权限	字符串
ssm:resourceTag/aws:ssmmessages:target-id	根据分配给 Systems Manager 会话资源的标签键/值对筛选访问权限	字符串
ssm:resourceTag/tag-key	根据分配给 Systems Manager 资源的标签键/值对筛选访问权限	字符串

Amazon Systems Manager GUI Connect 的操作、资源和条件键

Amazon Systems Manager GUI Connect（服务前缀:`ssm-guiconnect`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Systems Manager GUI Connect 定义的操作
- Amazon Systems Manager GUI Connect 定义的资源类型
- Amazon Systems Manager GUI Connect 的条件键

Amazon Systems Manager GUI Connect 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CancelConnection[仅权限]	授予权限以终止 GUI Connect 连接	写入			
GetConnection[仅权限]	授予权限以获取 GUI Connect 连接的元数据	读取			
ListConnections[仅权限]	授予权限以列出 GUI Connect 连接的元数据	列表			
StartConnection[仅权限]	授予权限以启动 GUI Connect 连接	写入			

Amazon Systems Manager GUI Connect 定义的资源类型

Amazon Systems Manager GUI Connect 不支持在 IAM 策略声明的`Resource`元素中指定资源 ARN。要允许访问 Amazon Systems Manager GUI Connect，请在策略中指定 `"Resource": "*"`。

Amazon Systems Manager GUI Connect 的条件键

GUI Connect 没有可在策略声明的 `Condition` 元素中使用的服务特定上下文键。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon Timestream InfluxDB 的操作、资源和条件键

Amazon Timestream InfluxDB（服务前缀：`timestream-influxdb`）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Timestream InfluxDB 定义的操作
- Amazon Timestream InfluxDB 定义的资源类型
- Amazon Timestream InfluxDB 的条件键

Amazon Timestream InfluxDB 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateDbCluster	授予创建新 Timestream InfluxDB 集群的权限	写入	db-parameter-group		timestream-influxdb:CreateDbInstance
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDbInstance	授予权限以创建新的 Timestream InfluxDB 实例	写入	db-parameter-group		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateDbParameterGroup	授予权限以创建新的 Timestream InfluxDB 参数组	写入		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDbCluster	授予删除 Timestream InfluxDB 集群的权限	写入	db-cluster*		timestream-influxdb:DeleteDbInstance
DeleteDbInstance	授予权限以删除 Timestream InfluxDB 实例	写入	db-instance*		
GetDbCluster	授予获取有关 Timestream InfluxDB 集群信息的权限	读取	db-cluster*		
GetDbInstance	授予权限以获取有关 Timestream InfluxDB 实例的信息	读取	db-instance*		
GetDbParameterGroup	授予权限以获取有关 Timestream InfluxDB 参数组的信息	读取	db-parameter-group*		
ListDbClusters	授予列出账户中所有 Timestream InfluxDB 集群信息的权限	列表			
ListDbInstances	授予权限以列出有关账户中所有 Timestream InfluxDB 实例的信息	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListDbInstancesForCluster	授予列出属于集群的所有 Timestream InfluxDB 实例信息的权限	读取	db-cluster*		
ListDbParameterGroups	授予权限以列出有关所有 Timestream InfluxDB 参数组的信息	列表			
ListTagsForResource	授予权限以列出 Timestream InfluxDB 资源的标签	读取	db-cluster		
			db-instance		
			db-parameter-group		
				aws:ResourceTag/${TagKey}	
TagResource	授予权限以标记 Timestream InfluxDB 资源	标记	db-cluster		
			db-instance		
			db-parameter-group		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	授予权限以取消标记 Timestream InfluxDB 资源	标记	db-cluster		
			db-instance		
			db-parameter-group		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateDbCluster	授予更新 Timestream InfluxDB 集群的权限	写入	db-cluster*		timestream-influxdb:UpdateDbInstance

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			db-parameter-group		
UpdateDbInstance	授予权限以更新 Timestream InfluxDB 实例	写入	db-instance*		
			db-parameter-group		

Amazon Timestream InfluxDB 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
db-cluster	arn:${Partition}:timestream-influxdb:${Region}:${Account}:db-cluster/${DbClusterId}	aws:ResourceTag/${TagKey}
db-instance	arn:${Partition}:timestream-influxdb:${Region}:${Account}:db-instance/${DbInstanceIdentifier}	aws:ResourceTag/${TagKey}
db-parameter-group	arn:${Partition}:timestream-influxdb:${Region}:${Account}:db-parameter-group/${DbParameterGroupIdentifier}	aws:ResourceTag/${TagKey}

Amazon Timestream InfluxDB 的条件键

Amazon Timestream InfluxDB 定义以下条件键，可在 IAM 策略的 Condition 元素中使用。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中允许的标签键值对筛选访问	字符串
aws:ResourceTag/${TagKey}	按某个资源的标签键值对筛选访问	字符串
aws:TagKeys	按请求中允许的标签键列表筛选访问	ArrayOfString

Amazon Transcribe 的操作、资源和条件键

Amazon Transcribe（服务前缀：transcribe）提供以下服务特定的资源、操作和条件上下文键以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Transcribe 定义的操作
- Amazon Transcribe 定义的资源类型
- Amazon Transcribe 的条件键

Amazon Transcribe 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateCallAnalyticsCategory	授予权限以创建分析类别。Amazon Transcribe 将按您的分析类别指定的条件应用于您的呼叫分析作业	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLanguageModel	授予权限以创建新的自定义语言模型	Write		aws:RequestTag/${TagKey}	s3:GetObject

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys	s3:ListBucket
CreateMedicalVocabulary	授予权限以创建新的自定义词汇表，可使用此词汇表更改 Amazon Transcribe Medical 处理音频文件转录的方式	Write		aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
CreateVocabulary	授予权限以创建新的自定义词汇表，可使用此词汇表更改 Amazon Transcribe 处理音频文件转录的方式	Write		aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
CreateVocabularyFilter	授予权限以创建一个新的词汇表筛选条件，可使用它从由 Amazon Transcribe 生成的音频文件的转录中筛选出单词	Write		aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
DeleteCallAnalyticsCategory	授予权限以使用 Amazon Transcribe 中的名称删除呼叫分析类别	Write	callanalyticscategory*		
DeleteCallAnalyticsJob	授予权限以删除以前提交的呼叫分析作业以及生成的任何其他结果，例如转录、模型等	Write	callanalyticsjob*		
DeleteLanguageModel	授予权限以删除先前创建的自定义语言模型	写入	languagemodel*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteMedicalScribeJob	授予删除之前提交的医疗抄写员作业的权限	写入	medicalscribejob*		
DeleteMedicalTranscriptionJob	授予权限以删除之前提交的医疗转录作业	Write	medicaltranscriptionjob*		
DeleteMedicalVocabulary	授予权限以从 Amazon Transcribe 中删除医学词汇表	Write	medicalvocabulary*		
DeleteTranscriptionJob	授予权限以删除以前提交的转录作业以及生成的任何其他结果，例如转录、模型等	Write	transcriptionjob*		
DeleteVocabulary	授予权限以从 Amazon Transcribe 中删除词汇表	Write	vocabulary*		
DeleteVocabularyFilter	授予权限以从 Amazon Transcribe 中删除词汇表筛选条件	Write	vocabularyfilter*		
DescribeLanguageModel	授予权限以返回有关自定义语言模型的信息	Read	languagemodel*		
GetCallAnalyticsCategory	授予权限以检索有关呼叫分析类别的信息	Read	callanalyticscategory*		
GetCallAnalyticsJob	授予权限以返回有关呼叫分析作业的信息	读取	callanalyticsjob*		
GetMedicalScribeJob	授予返回医疗抄写员作业信息的权限	读取	medicalscribejob*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetMedicalScribeStream	授予获取有关指定 Amazon HealthScribe 直播会话信息的权限	读取			
GetMedicalTranscriptionJob	授予权限以返回有关医疗转录作业的信息	Read	medicaltranscriptionjob*		
GetMedicalVocabulary	授予权限以获取有关医学词汇表的信息	Read	medicalvocabulary*		
GetTranscriptionJob	授予权限以返回有关转录作业的信息	Read	transcriptionjob*		
GetVocabulary	授予权限以获取有关词汇表的信息	Read	vocabulary*		
GetVocabularyFilter	授予权限以获取有关词汇表筛选条件的信息	Read	vocabularyfilter*		
ListCallAnalyticsCategories	授予权限以列出已创建的呼叫分析类别	List			
ListCallAnalyticsJobs	授予权限以列出具有指定状态的呼叫分析作业	List			
ListLanguageModels	授予权限以列出自定义语言模型	列表			
ListMedicalScribeJobs	授予列出具有指定状态的医疗抄写员作业的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListMedicalTranscriptionJobs	授予权限以列出具有指定状态的医疗转录作业	List			
ListMedicalVocabularies	授予权限以返回符合指定条件的医学词汇表的列表。如果未指定任何条件，则返回整个词汇表列表	列表			
ListTagsForResource	授予权限以列出资源的标签	读取			
ListTranscriptionJobs	授予权限以列出具有指定状态的转录作业	List			
ListVocabularies	授予权限以返回与指定条件匹配的词汇表列表。如果未指定任何条件，则返回整个词汇表列表	List			
ListVocabularyFilters	授予权限以返回符合指定条件的词汇表筛选条件的列表。如果未指定任何条件，则返回最多 5 个词汇表筛选器	List			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StartCallAnalyticsJob	授予权限以启动异步分析作业，该作业不仅转录来电人和客服的音频录制，而且还返回其他洞察	写入		transcribe:OutputEncryptionKMSKeyId transcribe:OutputLocation aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
StartCallAnalyticsStreamTranscription	授予权限以启动一个协议，其中音频将流式传输到 Transcribe Call Analytics，并且转录结果将流式传输到您的应用程序	写入			
StartCallAnalyticsStreamTranscriptionWebSocket	授予启动权限，将音频流式传输到 Transcribe Call Analytics，并将转录结果流式传输到您的应用程序 WebSocket	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StartMedicalScribeJob	授予启动异步作业以转录患者与临床医生的对话，并生成临床笔记的权限	写入		transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
StartMedicalScribeStream	授予启动双向流的权限，在该双向 HTTP2 流中，音频将流式传输到 Amazon HealthScribe 您的应用程序，并将转录结果流式传输到您的应用程序	写入			
StartMedicalStreamTranscription	授予权限以启动一个协议，其中音频将流式传输到 Transcribe Medical，并且转录结果将流式传输到您的应用程序	写入			
StartMedicalStreamTranscriptionWebSocket	授予启动将音频流式传输到 Transcribe Medical 并将转录结果流式传输到您的应用程序的权限 WebSocket	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StartMedicalTranscriptionJob	授予权限以启动异步作业以将医学语音转录为文本	写入		transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId transcribe:OutputKey aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
StartStreamTranscription	授予启动双向 HTTP2 直播以将语音实时转录为文本的权限	写入			
StartStreamTranscriptionWebSocket	授予权限以启动 Websocket 流以实时将语音转录为文本	Write			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StartTranscriptionJob	授予权限以启动异步作业以将语音转录为文本	写入		transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId transcribe:OutputKey aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
TagResource	授予权限以使用给定的键值对标记资源	Tagging		aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予权限以取消标记具有给定键的资源	标记		aws:TagKeys	
UpdateCallAnalyticsCategory	授予权限以使用新值更新呼叫分析类别。该 UpdateCallAnalyticsCategory 操作会使用您在请求中提供的值覆盖所有现有信息	写入	callanalyticscategory*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateMedicalVocabulary	授予权限以使用新值更新现有医学词汇表。该 UpdateMedicalVocabulary 操作会使用您在请求中提供的值覆盖所有现有信息	写入	medicalvocabulary*		s3:GetObject
UpdateVocabulary	授予权限以使用新值更新现有词汇表。该 UpdateVocabulary 操作会使用您在请求中提供的值覆盖所有现有信息	写入	vocabulary*		s3:GetObject
UpdateVocabularyFilter	授予权限以使用新值更新现有词汇表筛选条件。该 UpdateVocabularyFilter 操作会使用您在请求中提供的值覆盖所有现有信息	写入	vocabularyfilter*		s3:GetObject

Amazon Transcribe 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
transcriptionjob	arn:${Partition}:transcribe:${Region}:${Account}:transcription-job/${JobName}	aws:ResourceTag/${TagKey}
vocabulary	arn:${Partition}:transcribe:${Region}:${Account}:vocabulary/${VocabularyName}	aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
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}

Amazon Transcribe 的条件键

Amazon Transcribe 定义以下可以在 IAM policy 的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	通过要求资源创建请求中存在标签值来筛选访问权限	字符串
aws:ResourceTag/${TagKey}	通过要求提供与资源关联的标签值筛选访问权限	字符串
aws:TagKeys	通过要求请求中必需具有强制性标签来筛选访问权限	ArrayOfString
transcribe:OutputBucketName	基于请求中包含的输出存储桶名称筛选访问	字符串
transcribe:OutputEncryptionKMSKeyId	基于请求中包含的 KMS 密钥筛选访问	字符串
transcribe:OutputKey	请求中包含的输出密钥筛选访问	字符串
transcribe:OutputLocation	根据请求中包含的输出位置筛选访问	字符串

Amazon Transfer Family 的操作、资源和条件键

Amazon Transfer Family（服务前缀:`transfer`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Transfer Family 定义的操作
- Amazon Transfer Family 定义的资源类型
- Amazon Transfer Family 的条件键

Amazon Transfer Family 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateAccess	授予权限以添加与服务器关联的访问	写入	server*		iam:PassRole
CreateAgreement	授予权限以添加与服务器关联的协议	写入	server*		iam:PassRole

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateConnector	授予权限以创建连接器	写入		aws:TagKeys aws:RequestTag/${TagKey}	iam:PassRole
CreateProfile	授予创建配置文件的权限	写入		aws:TagKeys aws:RequestTag/${TagKey}	
CreateServer	授予权限以创建服务器	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:PassRole
CreateUser	授予添加与服务器关联的用户的权限	写入	server*		iam:PassRole

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateWebApp	授予创建 Web 应用程序的权限	写入		aws:TagKeys aws:RequestTag/${TagKey}	iam:PassRole
CreateWorkflow	授予权限以创建工作流程	写入		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteAccess	授予权限以删除访问	写入	server*		
DeleteAgreement	授予权限以删除协议	写入	agreement*		
DeleteCertificate	授予权限以删除证书	写入	certificate*		
DeleteConnector	授予权限以删除连接器	写入	connector*		
DeleteHostKey	授予删除与服务器关联的主机密钥的权限	写入	host-key*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteProfile	授予权限以删除配置文件	写入	profile*		
DeleteServer	授予删除服务器的权限	Write	server*		
DeleteSshPublicKey	授予从用户删除 SSH 公有密钥的权限	Write	user*		
DeleteUser	授予删除与服务器关联的用户的权限	写入	user*		
DeleteWebApp	授予删除 Web 应用程序的权限	写入	webapp*		
DeleteWebAppCustomization	授予删除 Web 应用程序自定义项的权限	写入	webapp*		
DeleteWorkflow	授予权限以删除工作流程	写入	workflow*		
DescribeAccess	授予权限以描述分配给服务器的访问	读取	server*		
DescribeAgreement	授予权限以描述分配给服务器的协议	读取	agreement*		
DescribeCertificate	授予权限以描述证书	读取	certificate*		
DescribeConnector	授予权限以描述连接器	读取	connector*		
DescribeExecution	授予权限以描述与工作流关联的执行情况	读取	workflow*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeHostKey	授予描述与服务器关联的主机密钥的权限	读取	host-key*		
DescribeProfile	授予权限以描述配置文件	读取	profile*		
DescribeSecurityPolicy	授予权限以描述安全策略	Read			
DescribeServer	授予描述服务器的权限	Read	server*		
DescribeUser	授予描述与服务器关联的用户的权限	读取	user*		
DescribeWebApp	授予描述 Web 应用程序的权限	读取	webapp*		
DescribeWebAppCustomization	授予描述 Web 应用程序自定义项的权限	读取	webapp*		
DescribeWorkflow	授予权限以描述工作流	读取	workflow*		
ImportCertificate	授予权限以添加证书	写入		aws:TagKeys aws:RequestTag/${TagKey}	
ImportHostKey	授予将主机密钥添加到服务器的权限	写入	server*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys aws:RequestTag/${TagKey}	
ImportSshPublicKey	授予向用户添加 SSH 公有密钥的权限	写入	user*		
ListAccesses	授予权限以列出访问	读取	server*		
ListAgreements	授予权限以列出协议	读取	server*		
ListCertificates	授予权限以列出证书	读取			
ListConnectors	授予权限以列出连接器	读取			
ListExecutions	授予权限以列出与工作流关联的执行情况	读取	workflow*		
ListFileTransferResults	授予权限以列出连接器的文件传输功能状态	读取	connector*		
ListHostKeys	授予列出与服务器关联的主机密钥的权限	读取	server*		
ListProfiles	授予列出配置文件的权限	读取			
ListSecurityPolicies	授予权限以列出安全策略	List			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListServers	授予列出服务器的权限	列表			
ListTagsForResource	授予列出 Transfer Family Amazon 资源标签的权限	读取	agreement		
			certificate		
			connector		
			host-key		
			profile		
			server		
			user		
			workflow		
ListUsers	授予列出与服务器关联的用户的权限	列表	server*		
ListWebApps	授予列出 Web 应用程序的权限	列表			
ListWorkflows	授予权限以列出工作流	列表			
SendWorkflowStepState	授予权限以为异步自定义步骤发送回调	写入	workflow*		
StartDirectoryListing	授予权限以使用连接器在远程服务器上启动列表操作	写入	connector*		
StartFileTransfer	授予启动连接器文件传输的权限	写入	connector*		
StartServer	授予权限以开启服务器	Write	server*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StopServer	授予停止服务器的权限	写入	server*		
TagResource	授予标记 Transfer F Amazon amily 资源的权限	标记	agreement		
			certificate		
			connector		
			host-key		
			profile		
			server		
			user		
			webapp		
			workflow		
				aws:TagKeys aws:RequestTag/${TagKey}	
TestConnection	授予权限以测试连接器与远程服务器的连接	写入	connector*		
TestIdentityProvider	授予测试服务器的自定义身份提供商的权限	读取	user*		
UntagResource	授予取消标记 Transfer Famil Amazon y 资源的权限	标记	agreement		
			certificate		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			connector		
			host-key		
			profile		
			server		
			user		
			webapp		
			workflow		
				aws:TagKeys	
UpdateAccess	授予权限以更新访问	写入			iam:PassRole
UpdateAgreement	授予权限以更新协议	写入	agreement*		iam:PassRole
UpdateCertificate	授予权限以更新证书	写入	certificate*		
UpdateConnector	授予权限以更新连接器	写入	connector*		iam:PassRole
UpdateHostKey	授予更新主机密钥的权限	写入	host-key*		
UpdateProfile	授予更新配置文件的权限	写入	profile*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateServer	授予权限以更新服务器配置	Write	server*		iam:PassRole
UpdateUser	授予更新用户配置的权限	写入	user*		iam:PassRole
UpdateWebApp	授予更新 Web 应用程序配置的权限	写入	webapp*		iam:PassRole
UpdateWebAppCustomization	授予更新 Web 应用程序自定义配置的权限	写入	webapp*		iam:PassRole

Amazon Transfer Family 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
user	arn:${Partition}:transfer:${Region}:${Account}:user/${ServerId}/${UserName}	aws:ResourceTag/${TagKey}
server	arn:${Partition}:transfer:${Region}:${Account}:server/${ServerId}	aws:ResourceTag/${TagKey}
workflow	arn:${Partition}:transfer:${Region}:${Account}:workflow/${WorkflowId}	aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
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}

Amazon Transfer Family 的条件键

Amazon Transfer Family 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串

条件键	描述	类型
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString

Amazon Trusted Advisor 的操作、资源和条件键

Amazon Trusted Advisor（服务前缀:`trustedadvisor`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon Trusted Advisor 定义的操作
- Amazon Trusted Advisor 定义的资源类型
- Amazon Trusted Advisor 的条件键

Amazon Trusted Advisor 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

> **Note**
>
> IAM Trusted Advisor 策略描述详细信息仅适用于 Trusted Advisor 控制台。如果要管理对 Trusted Advisor 的编程访问，请使用 Amazon Web Services 支持 API 中的 Trusted Advisor 操作。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchUpdateRecommendationResourceExclusion	授予权限以更新推荐资源列表的一个或多个排除状态	写入			
CreateEngagement	授予创建参与的权限	写入			
CreateEngagementAttachment	授予创建参与附件的权限	写入			
CreateEngagementCommunication	授予创建参与通信的权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteNotification ConfigurationForDelegatedAdmin	向组织管理账户授予权限，允许其从 Trusted Advisor Priority 的委托管理员账户中删除电子邮件通知首选项	写入			
DescribeAccount[仅权限]	授予查看 Amazon Web Services 支持 计划和各种 T Amazon rusted Advisor 首选项的权限	读取			
DescribeAccountAccess[仅权限]	授予查看是启用还是禁用 T Amazon rust Amazon Web Services 账户 ed Advisor 的权限	读取			
DescribeCheckItems	授予权限以查看检查项目的详细信息	读取	checks*		
DescribeCheckRefreshStatuses	授予查看 Truste Amazon d Advisor 检查刷新状态的权限	读取	checks*		
DescribeCheckStatusHistoryChanges[仅权限]	授予权限以查看过去 30 天内检查的结果和更改状态	读取	checks*		
DescribeCheckSummaries	授予查看 Tru Amazon sted Advisor 支票摘要的权限	读取	checks*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeChecks	授予查看 T Amazon rusted Advisor 支票详情的权限	读取			
DescribeNotificationConfigurations	授予权限以获取 Trusted Advisor Priority 的电子邮件通知首选项	读取			
DescribeNotificationPreferences[仅权限]	授予查看通知首选项的权限 Amazon Web Services 账户	读取			
DescribeOrganization[仅权限]	授予查看是否 Amazon Web Services 账户 满足启用组织视图功能的要求的权限	读取			
DescribeOrganizationAccounts[仅权限]	授予查看组织中关联 Amazon 账户的权限	读取			
DescribeReports[仅权限]	授予权限以查看组织视图报告的详细信息（例如，报告名称、运行时间、创建日期、状态和格式）	读取			
DescribeRisk	授予在 T Amazon rusted Advisor 优先级中查看风险详细信息的权限	读取			
DescribeRiskResources	授予在 Truste Amazon d Advisor 优先级中查看受影响资源的权限	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeRisks	授予在 T Amazon rusted Advisor 优先级中查看风险的权限	读取			
DescribeServiceMetadata[仅权限]	授予查看组织视图报告相关信息的权限，例如支票类别、支票名称和资源状态 Amazon Web Services 区域	读取			
DownloadRisk	授予下载包含 T Amazon rusted Advisor 优先级风险详细信息的文件的权限	读取			
ExcludeCheckItems[仅权限]	授予排除针对 T Amazon rusted Advisor 支票的推荐的权限	写入	checks*		
GenerateReport[仅权限]	授予为组织中的 T Amazon rusted Advisor 支票创建报告的权限	写入			
GetEngagement	授予查看参与的权限	读取			
GetEngagementAttachment	授予查看参与附件的权限	读取			
GetEngagementType	授予查看特定参与类型的权限	读取			
GetOrganizationRecommendation	授予在 Amazon 组织组织内获得特定推荐的权限。此 API 仅支持按优先顺序排列的建议	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetRecommendation	授予获取特定建议的权限	读取			
IncludeCheckItems[仅权限]	授予包含针对 T Amazon rusted Advisor 支票的建议的权限	写入	checks*		
ListAccountsForParent[仅权限]	授予在 Trusted Advisor 控制台中查看 Amazon 组织中由根或组织单位 (OU) 包含的所有账户的权限	读取			
ListChecks	授予列出可筛选的检查集的权限	列表			
ListEngagementCommunications	授予查看所有参与通信的权限	读取			
ListEngagementTypes	授予查看所有参与类型的权限	读取			
ListEngagements	授予查看所有参与的权限	读取			
ListOrganizationRecommendationAccounts	授予列出拥有 Amazon 组织汇总推荐资源的账户的权限。此 API 仅支持按优先顺序排列的建议	列表			
ListOrganizationRecommendationResources	授予在 Amazon 组织内列出推荐资源的权限。此 API 仅支持按优先顺序排列的建议	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListOrganizationRecommendations	授予在组织内列出一组可筛选的推荐的权限。 Amazon 此 API 仅支持按优先顺序排列的建议	列表			
ListOrganizationalUnitsForParent[仅权限]	授予在 Trusted Advisor 控制台中查看上级组织单位或根目录中所有组织单位 (OUs) 的权限	读取			
ListRecommendationResources	授予列出建议的资源的权限	列表			
ListRecommendations	授予列出可筛选建议集的权限	列表			
ListRoots[仅权限]	授予在 Trusted Advisor 控制台中查看 Amazon 组织中定义的所有根目录的权限	读取			
RefreshCheck	授予刷新 Tru Amazon sted Advisor 支票的权限	写入	checks*		
SetAccountAccess[仅权限]	授予为账户启用或禁用 T Amazon rusted Advisor 的权限	写入			
SetOrganizationAccess[仅权限]	授予为 T Amazon rusted Advisor 启用组织视图功能的权限	写入			
UpdateEngagement	授予权限以更新参与的详细信息	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateEngagementStatus	授予更新参与状态的权限	写入			
UpdateNotificationConfigurations	授予权限以创建或更新 Trusted Advisor Priority 的电子邮件通知首选项	写入			
UpdateNotificationPreferences[仅权限]	授予更新 T Amazon rusted Advisor 通知首选项的权限	写入			
UpdateOrganizationRecommendationLifecycle	授予在 Amazon 组织内更新建议生命周期的权限。此 API 仅支持按优先顺序排列的建议	写入			
UpdateRecommendationLifecycle	授予更新建议的生命周期的权限。此 API 仅支持按优先顺序排列的建议	写入			
UpdateRiskStatus	授予在 T Amazon rusted Advisor 优先级中更新风险状态的权限	写入			

Amazon Trusted Advisor 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

> **Note**
>
> 支票资源类型的 ARN 不应包括区域。在格式中使用“*”而不是“${Region}”，否则策略将无法正常工作。

资源类型	ARN	条件键
checks	`arn:${Partition}:trustedadvisor:${Region}:${Account}:checks/${CategoryCode}/${CheckId}`	

Amazon Trusted Advisor 的条件键

Trusted Advisor 没有可以在策略语句的 `Condition` 元素中使用的服务特定上下文键。有关适用于所有服务的全局上下文键列表，请参阅可用的条件键。

Amazon WAF Regional 的操作、资源和条件键

Amazon WAF Regional（服务前缀:`waf-regional`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon WAF Regional 定义的操作
- Amazon WAF Regional 定义的资源类型
- Amazon WAF Regional 的条件键

Amazon WAF Regional 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateWebACL	授予将 WebACL 与资源关联的权限	写入	loadbalancer/app/*		
			webacl*		
CreateByteMatchSet	授予创建 ByteMatchSet	写入	bytematchset*		
CreateGeoMatchSet	授予创建 GeoMatchSet	写入	geomatchset*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateIPSet	授予创建 IPSet	写入	ipset*		
CreateRateBasedRule	授予创建 RateBasedRule	写入	ratebasedrule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRegexMatchSet	授予创建 RegexMatchSet	写入	regexmatchset*		
CreateRegexPatternSet	授予创建 RegexPatternSet	写入	regexpatternset*		
CreateRule	授予创建规则的权限	写入	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleGroup	授予创建 RuleGroup	写入	rulegroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateSizeConstraintSet	授予创建 SizeConstraintSet	写入	sizeconstraintset*		
CreateSqlInjectionMatchSet	授予创建 SqlInjectionMatchSet	写入	sqlinjectionmatchset*		
CreateWebACL	授予创建 WebACL 的权限	权限管理	webacl*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebACLMigrationStack	授予在 S3 存储桶中创建 CloudFormation Web ACL 模板的权限，以便将 Web ACL 从 Amazon WAF Classic 迁移到 W Amazon AF v2	写入	webacl*		s3:PutObject
CreateXssMatchSet	授予创建 XssMatchSet	写入	xssmatchset*		
DeleteByteMatchSet	授予删除权限 ByteMatchSet	写入	bytematchset*		
DeleteGeoMatchSet	授予删除权限 GeoMatchSet	写入	geomatchset*		
DeleteIPSet	授予删除的权限 IPSet	写入	ipset*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteLoggingConfiguration	授予 LoggingConfiguration 从 Web ACL 中删除的权限	写入	webacl*		
DeletePermissionPolicy	授予从规则组中删除 IAM policy 的权限	权限管理	rulegroup*		
DeleteRateBasedRule	授予删除权限 RateBasedRule	写入	ratebasedrule*		
DeleteRegexMatchSet	授予删除权限 RegexMatchSet	写入	regexmatchset*		
DeleteRegexPatternSet	授予删除权限 RegexPatternSet	写入	regexpatternset*		
DeleteRule	授予删除规则的权限	写入	rule*		
DeleteRuleGroup	授予删除权限 RuleGroup	写入	rulegroup*		
DeleteSizeConstraintSet	授予删除权限 SizeConstraintSet	写入	sizeconstraintset*		
DeleteSqlInjectionMatchSet	授予删除的权限 SqlInjectionMatchSet	写入	sqlinjectionmatchset*		
DeleteWebACL	授予删除 WebACL 的权限	权限管理	webacl*		
DeleteXssMatchSet	授予删除的权限 XssMatchSet	写入	xssmatchset*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DisassociateWebACL	授予删除 Web ACL 和资源之间关联的权限	写入	loadbalancer/app/*		
GetByteMatchSet	授予检索权限 ByteMatchSet	读取	bytematchset*		
GetChangeToken	授予检索要在创建、更新和删除请求中使用的更改令牌的权限	Read			
GetChangeTokenStatus	授予检索更改令牌状态的权限	读取			
GetGeoMatchSet	授予检索权限 GeoMatchSet	读取	geomatchset*		
GetIPSet	授予检索权限 IPSet	读取	ipset*		
GetLoggingConfiguration	授予检索权限 LoggingConfiguration	读取	webacl*		
GetPermissionPolicy	授予检索附加到的 IAM 策略的权限 RuleGroup	读取	rulegroup*		
GetRateBasedRule	授予检索权限 RateBasedRule	读取	ratebasedrule*		
GetRateBasedRuleManagedKeys	授予检索当前被屏蔽的 IP 地址数组的权限 RateBasedRule	读取	ratebasedrule*		
GetRegexMatchSet	授予检索权限 RegexMatchSet	读取	regexmatchset*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetRegexPatternSet	授予检索权限 RegexPatternSet	读取	regexpatternset*		
GetRule	授予检索规则的权限	读取	rule*		
GetRuleGroup	授予检索权限 RuleGroup	读取	rulegroup*		
GetSampledRequests	授予检索 Web 请求示例集的详细信息的权限	读取	webacl		
GetSizeConstraintSet	授予检索权限 SizeConstraintSet	读取	sizeconstraintset*		
GetSqlInjectionMatchSet	授予检索权限 SqlInjectionMatchSet	读取	sqlinjectionmatchset*		
GetWebACL	授予检索 WebACL 的权限	Read	webacl*		
GetWebACLForResource	授予检索与指定资源关联的 WebACL 的权限	读取	loadbalancer/app/*		
GetXssMatchSet	授予检索权限 XssMatchSet	读取	xssmatchset*		
ListActivatedRulesInRuleGroup	授予检索 ActivatedRule 对象数组的权限	列表			
ListByteMatchSets	授予检索 ByteMatchSetSummary 对象数组的权限	列表			
ListGeoMatchSets	授予检索 GeoMatchSetSummary 对象数组的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListIPSets	授予检索 IPSet摘要对象数组的权限	列表			
ListLoggingConfigurations	授予检索 LoggingConfiguration 对象数组的权限	列表			
ListRateBasedRules	授予检索 RuleSummary 对象数组的权限	列表			
ListRegexMatchSets	授予检索 RegexMatchSetSummary 对象数组的权限	列表			
ListRegexPatternSets	授予检索 RegexPatternSetSummary 对象数组的权限	列表			
ListResourcesForWebACL	授予检索与指定 WebACL 关联的资源阵列的权限	列表	webacl*		
ListRuleGroups	授予检索 RuleGroup 对象数组的权限	列表			
ListRules	授予检索 RuleSummary 对象数组的权限	列表			
ListSizeConstraintSets	授予检索 SizeConstraintSetSummary 对象数组的权限	列表			
ListSqlInjectionMatchSets	授予检索 SqlInjectionMatchSet 对象数组的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListSubscribedRuleGroups	授予检索您订阅的 RuleGroup 对象数组的权限	列表			
ListTagsForResource	授予列出资源标签的权限	读取	ratebasedrule		
			rule		
			rulegroup		
			webacl		
ListWebACLs	授予检索 Web ACLSummary 对象数组的权限	列表			
ListXssMatchSets	授予检索 XssMatchSet 对象数组的权限	列表			
PutLoggingConfiguration	授予将 LoggingConfiguration 与 Web ACL 关联的权限	写入	webacl*		iam:CreateServiceLinkedRole
PutPermissionPolicy	授予将 IAM policy 附加到指定规则组，以支持账户之间规则组共享的权限	Permissions management	rulegroup*		
TagResource	授予将标签添加到资源的权限	Tagging	ratebasedrule		
			rule		
			rulegroup		
			webacl		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予从资源中删除标签的权限	标记	ratebasedrule		
			rule		
			rulegroup		
			webacl		
				aws:TagKeys	
UpdateByteMatchSet	授予在中插入或删除 ByteMatchTuple 对象的权限 ByteMatchSet	写入	bytematchset*		
UpdateGeoMatchSet	授予在中插入或删除 GeoMatchConstraint 对象的权限 GeoMatchSet	写入	geomatchset*		
UpdateIPSet	授予在中插入或删除 IPSet描述符对象的权限 IPSet	写入	ipset*		
UpdateRateBasedRule	授予在基于费率的规则中插入或删除谓词对象以及更新规则 RateLimit 中的谓词对象的权限	写入	ratebasedrule*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateRegexMatchSet	授予在中插入或删除 RegexMatchTuple 对象的权限 RegexMatchSet	写入	regexmatchset*		
UpdateRegexPatternSet	授予在中插入或删除 RegexPatternStrings 的权限 RegexPatternSet	写入	regexpatternset*		
UpdateRule	授予在规则中插入或删除谓词对象的权限	写入	rule*		
UpdateRuleGroup	授予在中插入或删除 Activated Rule 对象的权限 RuleGroup	写入	rulegroup*		
UpdateSizeConstraintSet	授予在中插入或删除 SizeConstraint 对象的权限 SizeConstraintSet	写入	sizeconstraintset*		
UpdateSqlInjectionMatchSet	授予在中插入或删除 SqlInjectionMatchTuple 对象的权限 SqlInjectionMatchSet	写入	sqlinjectionmatchset*		
UpdateWebACL	授予在 WebACL 中插入或删除 ActivatedRule 对象的权限	权限管理	webacl*		
UpdateXssMatchSet	授予在中插入或删除 XssMatchTuple 对象的权限 XssMatchSet	写入	xssmatchset*		

Amazon WAF Regional 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从

而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}	

资源类型	ARN	条件键
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}

Amazon WAF Regional 的条件键

Amazon WAF Regional 定义了以下条件键，这些条件键可用于 IAM 策略的Condition元素。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据每个标签的允许值集筛选操作	字符串
aws:ResourceTag/${TagKey}	根据与资源关联的标签值筛选操作	字符串
aws:TagKeys	根据在请求中是否具有必需标签以筛选操作	ArrayOfString

Amazon WAF V2 的操作、资源和条件键

Amazon WAF V2（服务前缀:wafv2）提供以下特定于服务的资源、操作和条件上下文密钥以在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。

- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon WAF V2 定义的操作
- Amazon WAF V2 定义的资源类型
- Amazon WAF V2 的条件键

Amazon WAF V2 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
Associate WebACL	授予权限以将 WebACL 与资源关联。	Write	webacl*		apigateway:SetWebACL apprunner:AssociateWebAcl appsync:SetWebACL cognito-idp:AssociateWebACL ec2:AssociateVerifiedAccessInstanceWebAcl elasticloadbalancing:SetWebAcl
			apigateway		
			apprunner		
			appsync		
			loadbalancer/app/		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			userpool		
			verified-access-instance		
CheckCapacity	授予权限以计算指定范围和规则集的 Web ACL 容量单位 (WCU) 要求。	读取			
CreateAPIKey	授予创建 API 密钥的权限，以便在客户端应用程序中集成 CAPTCHA API 时使用 JavaScript	写入			
CreateIPSet	授予创建 IPSet	写入	ipset*		wafv2:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRegexPatternSet	授予创建 RegexPatternSet	写入	regexpatternset*		wafv2:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateRuleGroup	授予创建 RuleGroup	写入	rulegroup*		wafv2:TagResource
			ipset		
			regexpatternset		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebACL	授予创建 WebACL 的权限	写入	webacl*		wafv2:TagResource
			ipset		
			managedruleset		
			regexpatternset		
			rulegroup		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteAPIKey	授予删除 API 密钥的权限	写入			
DeleteFirewallManagerRuleGroups	如果不再由 Firewall Manager 管理，则授予 FirewallManagedRulesGroups 从 WebACL 中删除的权限	写入	webacl*		
DeleteIPSet	授予删除的权限 IPSet	写入	ipset*		
DeleteLoggingConfiguration	授予 LoggingConfiguration 从 WebACL 中删除的权限	写入	webacl*		
				wafv2:LogScope	
DeletePermissionPolicy	授予在 PermissionPolicy 上删除的权限 RuleGroup	权限管理	rulegroup*		
DeleteRegexPatternSet	授予删除权限 RegexPatternSet	写入	regexpatternset*		
DeleteRuleGroup	授予删除权限 RuleGroup	写入	rulegroup*		
DeleteWebACL	授予删除 WebACL 的权限	写入	webacl*		
DescribeAllManagedProducts	授予权限以检索托管规则组的产品信息	读取			
DescribeManagedProductsByVendor	授予权限以按给定供应商检索托管规则组的产品信息	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeManagedRuleGroup	授予权限以查看托管规则组的高级信息。	读取			
DisassociateFirewallManager[仅权限]	授予权限以取消 Firewall Manager 与 WebACL 的关联	写入	webacl*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DisassociateWebACL	授予权限以取消 WebACL 与应用程序资源的关联	写入	apigateway		apigateway:SetWebACL apprunner:DisassociateWebAcl appsync:SetWebACL cognito-idp:DisassociateWebACL ec2:DisassociateVerifiedAccessInstanceWebAcl elasticloadbalancing:SetWebAcl
			apprunner		
			appsync		
			loadbalancer/app/		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			userpool		
			verified-access-instance		
GenerateMobileSdkReleaseUrl	授予权限以为指定版本的移动 SDK 生成预签名下载 URL	读取			
GetDecryptedAPIKey	授予以解密状态返回 API 密钥的权限。使用此权限查看为密钥定义的令牌域	读取			
GetIPSet	授予检索相关详细信息的权限 IPSet	读取	ipset*		
				aws:ResourceTag/${TagKey}	
GetLoggingConfiguration	授予检索 Web LoggingConfiguration ACL 的权限	读取	webacl*		
				aws:ResourceTag/${TagKey} wafv2:LogScope	
GetManagedRuleSet	授予检索有关 a 的详细信息的权限 ManagedRuleSet	读取	managedruleset*		
GetMobileSdkRelease	授予权限以检索指定版本的移动 SDK 的信息，包括版本注释和标签	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetPermissionPolicy	授予检索 a PermissionPolicy 的权限 RuleGroup	读取	rulegroup*		
GetRateBasedStatementManagedKeys	授予权限以查看基于速率的规则当前阻止的键。	读取	webacl*		
				aws:ResourceTag/${TagKey}	
GetRegexPatternSet	授予检索有关 a 的详细信息的权限 RegexPatternSet	读取	regexpatternset*		
				aws:ResourceTag/${TagKey}	
GetRuleGroup	授予检索有关 a 的详细信息的权限 RuleGroup	读取	rulegroup*		
				aws:ResourceTag/${TagKey}	
GetSampledRequests	授予检索有关 Web 请求采样的详细信息的权限	Read	webacl*		
GetWebACL	授予检索 WebACL 详细信息的权限	Read	webacl*		
				aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetWebACLForResource	授予检索与资源关联的 WebACL 的权限	读取	webacl*		apprunner:DescribeWebAclForService cognito-idp:GetWebACLForResource ec2:GetVerifiedAccessInstanceWebAcl wafv2:GetWebACL
			apigateway		
			apprunner		
			appsync		
			loadbalancer/app/		
			userpool		
			verified-access-instance		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListAPIKeys	授予检索为指定范围定义的 API 密钥列表的权限	列表			
ListAvailableManagedRuleGroupVersions	授予检索可供您使用的托管规则组版本阵列的权限	列表			
ListAvailableManagedRuleGroups	授予权限以查看可供您使用的托管规则组数组。	列表			
ListIPSets	授予权限以检索您管理的 IP 集的 IPSet摘要对象数组	列表			
ListLoggingConfigurations	授予检索 LoggingConfiguration 对象数组的权限	列表		wafv2:LogScope	
ListManagedRuleSets	授予检索 ManagedRuleSet 对象数组的权限	列表			
ListMobileSdkReleases	授予权限以检索移动 SDK 和指定设备平台可用版本列表	列表			
ListRegexPatternSets	授予为你管理的正则表达式模式集检索 RegexPatternSetSummary 对象数组的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ListResourcesForWebACL	授予权限以检索与网页 ACL 关联的资源的 Amazon 资源名称数组 (ARNs)	列表	webacl*		apprunner:ListAssociatedServicesForWebAcl cognito-idp:ListResourcesForWebACL ec2:DescribeVerifiedAccessInstanceWebAclAssociations
			apprunner		
			userpool		
			verified-access-instance		
ListRuleGroups	授予您管理的规则组检索 RuleGroupSummary 对象数组的权限	列表			
ListTagsForResource	授予权限以列出资源的标签	读取	ipset		
			regexpatternset		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			rulegroup		
			webacl		
				aws:ResourceTag/${TagKey}	
ListWebACLs	授予为你管理的 Web 检索一组 Web ACLSummary 对象 ACLs 的权限	列表			
PutFirewallManagerRuleGroups[仅权限]	授予在 WebACL FirewallManagedRulesGroups 中创建的权限	写入	webacl*		
PutLoggingConfiguration	授予启用 LoggingConfiguration、开始记录 Web ACL 的权限	写入	webacl*		iam:CreateServiceLinkedRole
				wafv2:LogScope wafv2:LogDestinationResource	
PutManagedRuleSetVersions	授予允许创建新版本或更新现有版本的权限 ManagedRuleSet	写入	managedruleset*		
			rulegroup*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutPermissionPolicy	授予将 IAM policy 附加到资源，以用于在账户之间共享规则组的权限	权限管理	rulegroup *		
TagResource	授予将标签与 Amazon 资源关联的权限	标记	ipset		
			regexpatternset		
			rulegroup		
			webacl		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	授予取消标签与资源的关联的 Amazon 权限	标记	ipset		
			regexpatternset		
			rulegroup		
			webacl		
				aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateIPSet	授予更新权限 IPSet	写入	ipset*		
				aws:ResourceTag/${TagKey}	
UpdateManagedRuleSetVersionExpiryDate	授予更新版本到期日期的权限 ManagedRuleSet	写入	managedruleset*		
UpdateRegexPatternSet	授予更新权限 RegexPatternSet	写入	regexpatternset*		
				aws:ResourceTag/${TagKey}	
UpdateRuleGroup	授予更新权限 RuleGroup	写入	rulegroup*		
			ipset		
			regexpatternset		
				aws:ResourceTag/${TagKey}	
UpdateWebACL	授予权限以更新 WebACL	写入	webacl*		
			ipset		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
			managedruleset		
			regexpatternset		
			rulegroup		
				aws:ResourceTag/${TagKey}	

Amazon WAF V2 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 Resource 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}	

资源类型	ARN	条件键
rulegroup	arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/rulegroup/${Name}/${Id}	aws:ResourceTag/${TagKey}
regexpatternset	arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/regexpatternset/${Name}/${Id}	aws:ResourceTag/${TagKey}
loadbalancer/app/	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/app/${LoadBalancerName}/${LoadBalancerId}	
apigateway	arn:${Partition}:apigateway:${Region}::/restapis/${ApiId}/stages/${StageName}	
appsync	arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}	
userpool	arn:${Partition}:cognito-idp:${Region}:${Account}:userpool/${UserPoolId}	
apprunner	arn:${Partition}:apprunner:${Region}:${Account}:service/${ServiceName}/${ServiceId}	
verified-access-instance	arn:${Partition}:ec2:${Region}:${Account}:verified-access-instance/${VerifiedAccessInstanceId}	

Amazon WAF V2 的条件键

Amazon WAF V2 定义了以下可在 IAM 策略Condition元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按每个标签的允许值集筛选访问	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签值筛选访问权限	字符串
aws:TagKeys	按请求中是否具有必需标签来筛选访问	ArrayOfString
wafv2:LogDestinationResource	按日志目标 ARN 筛选访问权限 API PutLoggingConfiguration	ARN
wafv2:LogScope	按 Logging Configuration API 的日志范围筛选访问权限	字符串

Amazon 的操作、资源和条件密钥 WorkSpaces

Amazon WorkSpaces （服务前缀:`workspaces`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon 定义的操作 WorkSpaces
- Amazon 定义的资源类型 WorkSpaces
- Amazon 的条件密钥 WorkSpaces

Amazon 定义的操作 WorkSpaces

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AcceptAccountLinkInvitation	授予接受来自其他 Amazon 账户的邀请以共享 WorkSpaces BYOL 相同配置的权限	写入			
AssociateConnectionAlias	授予将连接别名与目录关联的权限	Write	connectionalias*		
			directoryid*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
AssociateIpGroups	授予将 IP 访问控制组与目录关联的权限	写入	directoryid*		
			workspaceipgroup*		
AssociateWorkspaceApplication	授予将工作空间应用程序与关联的权限 WorkSpace	写入	workspaceapplication*		
			workspaceid*		
				aws:ResourceTag/${TagKey}	
AuthorizeIpRules	授予向 IP 访问控制组添加规则的权限	写入	workspaceipgroup*		workspaces:UpdateRulesOfIpGroup
CopyWorkspaceImage	授予复制 WorkSpace 图像的权限	写入	workspaceimage*		workspaces:DescribeWorkspaceImages
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateAccountLinkInvitation	授予邀请其他 Amazon 账户共享 WorkSpaces BYOL 相同配置的权限	写入			
CreateConnectClientAddIn	授予在目录内创建 Amazon Connect 客户端插件的权限	写入	directory id*		
CreateConnectionAlias	授予创建连接别名以用于跨区域重定向的权限	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateIpGroup	授予创建 IP 访问控制组的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	
CreateStandbyWorkspaces	授予创建一个或多个备用服务器的权限 WorkSpaces	写入	directory id*		
			workspace id*		
				aws:RequestTag/${TagKey} aws:TagKeys	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateTags	授予为 WorkSpaces 资源创建标签的权限	标记		aws:RequestTag/${TagKey} aws:TagKeys	
CreateUpdatedWorkspaceImage	授予创建更新 WorkSpace 图像的权限	写入	workspaceimage*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspaceBundle	授予创建 WorkSpace 捆绑包的权限	写入	workspacebundle*		workspaces:CreateTags
			workspaceimage*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspaceImage	授予创建新 WorkSpace 图像的权限	写入	workspaceid*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspaces	授予创建一个或多个的权限 WorkSpaces	写入	directory id*		
			workspacebundle*		
			workspace id*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspacesPool	授予创建 WorkSpaces 池的权限	写入	directory id*		
			workspacebundle*		
			workspacespoolid*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccountLinkInvitation	授予删除邀请其他 Amazon 账户共享相同的 WorkSpaces BYOL 配置的权限	写入			
DeleteClientBranding	授予删除目录中 Amazon WorkSpaces 客户品牌数据的权限	写入	directoryid*		
DeleteConnectClientAddIn	授予删除目录内配置的 Amazon Connect 客户端插件的权限	写入	directoryid*		
DeleteConnectionAlias	授予删除连接别名的权限	Write	connectionalias*		
DeleteIpGroup	授予删除 IP 访问控制组的权限	写入	workspaceipgroup*		
DeleteTags	授予从 WorkSpaces 资源中删除标签的权限	标记		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteWorkspaceBundle	授予删除 WorkSpace 捆绑包的权限	写入	workspacebundle*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteWorkspaceImage	授予删除 WorkSpace 图像的权限	写入	workspaceimage*		
DeployWorkspaceApplications	授予在上部署所有待处理的工作空间应用程序的权限 WorkSpace	写入	workspaceid*		
				aws:ResourceTag/${TagKey}	
DeregisterWorkspaceDirectory	授予取消注册目录以使其无法在 Amazon 上使用的权限 WorkSpaces	写入	directoryid*		
DescribeAccount	授予检索账户自带许可证 (BYOL) 配置的 WorkSpaces 权限	读取			
DescribeAccountModifications	授予权限以检索对账户自带许可证 (BYOL) 配置的 WorkSpaces 修改	读取			
DescribeApplicationAssociations	授予检索与 WorkSpace 应用程序关联的资源信息的权限	列表	workspaceapplication*		
				aws:ResourceTag/${TagKey}	
DescribeApplications	授予获取 WorkSpace 应用程序信息的权限	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeBundleAssociations	授予检索与 WorkSpace 捆绑包关联的资源信息的权限	列表	workspacebundle*		
				aws:ResourceTag/${TagKey}	
DescribeClientBranding	授予在目录中检索 Amazon WorkSpaces 客户品牌数据的权限	读取	directoryid*		
DescribeClientProperties	授予检索 WorkSpaces 客户信息的权限	列表	directoryid*		
DescribeConnectClientAddIns	授予检索已创建的 Amazon Connect 客户端插件列表的权限	列表	directoryid*		
DescribeConnectionAliasPermissions	授予权限以检索连接别名的所有者授予其他 Amazon 账户的连接别名权限	读取	connectionalias*		
DescribeConnectionAliases	授予检索描述用于跨区域重定向的连接别名的列表的权限	读取			
DescribeImageAssociations	授予检索与 WorkSpace 图像关联的资源信息的权限	列表	workspaceimage*		
				aws:ResourceTag/${TagKey}	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeIpGroups	授予权限以检索有关 IP 访问控制组的信息	读取	workspaceipgroup*		
DescribeTags	授予描述 WorkSpaces 资源标签的权限	读取			
DescribeWorkspaceAssociations	授予检索与关联的资源信息的权限 WorkSpace	列表	workspaceid*		
				aws:ResourceTag/${TagKey}	
DescribeWorkspaceBundles	授予获取 WorkSpace 捆绑包相关信息的权限	列表			
DescribeWorkspaceDirectories	授予权限以检索注册到的目录的相关信息 WorkSpaces	读取			
DescribeWorkspaceImagePermissions	授予检索 WorkSpace 图片权限相关信息的权限	读取	workspaceimage*		
DescribeWorkspaceImages	授予检索 WorkSpace 图像相关信息的权限	列表			
DescribeWorkspaceSnapshots	授予检索 WorkSpace 快照相关信息的权限	列表	workspaceid*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DescribeWorkspaces	授予获取相关信息的权限 WorkSpaces	列表			
DescribeWorkspacesConnectionStatus	授予获取连接状态的权限 WorkSpaces	读取			
DescribeWorkspacesPoolSessions	授予检索 WorkSpaces 池会话相关信息的权限	列表	workspacespoolid*		
DescribeWorkspacesPools	授予检索 WorkSpaces 池相关信息的权限	列表			
DisassociateConnectionAlias	授予取消连接别名与目录的关联的权限	Write	connectionalias*		
DisassociateIpGroups	授予取消 IP 访问控制组与目录的关联的权限	写入	directoryid*		
			workspaceipgroup*		
DisassociateWorkspaceApplication	授予解除工作空间应用程序与工作空间应用程序关联的权限 WorkSpace	写入	workspaceapplication*		
			workspaceid*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey}	
GetAccountLink	授予检索与其他 Amazon 账户的链接以共享 WorkSpaces BYOL 配置的权限	读取			
ImportClientBranding	授予在目录中导入 Amazon WorkSpaces 客户品牌数据的权限	写入	directory id*		
ImportWorkspaceImage	授予将自带许可 (BYOL) 图片导入亚马逊的权限 WorkSpaces	写入			ec2:DescribeImages ec2:ModifyImageAttribute
ListAccountLinks	授予权限以检索与您共享您的 WorkSpaces BYOL 配置的 Amazon 账户的链接	列表			
ListAvailableManagementCidrRanges	授予列出可用 CIDR 范围的权限，以便为账户启用自带许可证 (BYOL) WorkSpaces	列表			
MigrateWorkspace	授予迁移权限 WorkSpaces	写入	workspacebundle*		
			workspace id*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ModifyAccount	授予修改账户自带许可证 (BYOL) 配置的 WorkSpaces 权限	写入			
ModifyCertificateBasedAuthProperties	授予权限以修改目录的基于证书的授权属性	写入	directory id*		
ModifyClientProperties	授予修改 WorkSpaces 客户机属性的权限	写入	directory id*		
ModifyEndpointEncryptionMode	授予在标准 TLS 和 FIPS 140-2 验证模式之间配置指定目录的权限	写入	directory id*		
ModifySamlProperties	授予权限以修改目录的 SAML 属性	写入	directory id*		
ModifySelfservicePermissions	授予修改用户自助服务 WorkSpace 管理功能的权限	权限管理	directory id*		
ModifyStreamingProperties	授予权限以修改流属性	写入	directory id*		
ModifyWorkspaceAccessProperties	授予权限以指定用户可以使用哪些设备和操作系统来访问他们的 WorkSpaces	写入	directory id*		
ModifyWorkspaceCreationProperties	授予修改用于创建的默认属性的权限 WorkSpaces	写入	directory id*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
ModifyWorkspaceProperties	授予修改 WorkSpace 属性的权限，包括运行模式和 AutoStop 周期	写入	workspaceid*		
ModifyWorkspaceState	授予修改状态的权限 WorkSpaces	写入	workspaceid*		
RebootWorkspaces	授予重启权限 WorkSpaces	写入	workspaceid*		
RebuildWorkspaces	授予重建权限 WorkSpaces	写入	workspaceid*		
RegisterWorkspaceDirectory	授予注册目录以便在 Amazon 上使用的权限 WorkSpaces	写入	directoryid*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RejectAccountLinkInvitation	授予拒绝来自其他 Amazon 账户的 WorkSpaces BYOL 共享相同配置的邀请的权限	写入			
RestoreWorkspace	授予恢复权限 WorkSpaces	写入	workspaceid*		
RevokeIpRules	授予从 IP 访问控制组中删除规则的权限	写入	workspaceipgroup*		workspaces:UpdateRulesOfIpGroup

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
StartWorkspaces	授予启动权限 AutoStop WorkSpaces	写入	workspaceid*		
StartWorkspacesPool	授予启动 WorkSpaces 池的权限	写入	workspacespoolid*		
StopWorkspaces	授予停止权限 AutoStop WorkSpaces	写入	workspaceid*		
StopWorkspacesPool	授予停止 WorkSpaces 池的权限	写入	workspacespoolid*		
Stream	向联合用户授予使用现有凭证登录和流式传输 WorkSpace 的权限	写入	directoryid*		
				workspaces:userId	
TerminateWorkspaces	授予终止权限 WorkSpaces	写入	workspaceid*		
TerminateWorkspacesPool	授予终止 WorkSpaces 池的权限	写入	workspacespoolid*		
TerminateWorkspacesPoolSession	授予终止 WorkSpaces 池会话的权限	写入			
UpdateConnectClientAddIn	授予更新 Amazon Connect 客户端插件的权限。使用此操作更新 Amazon Connect 客户端插件的名称和端点 URL	写入	directoryid*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateConnectionAliasPermission	授予与其他账户共享或取消共享连接别名的权限	Permissions management	connectionalias*		
UpdateRulesOfIpGroup	授予替换 IP 访问控制组规则的权限	写入	workspaceipgroup*		workspaces:AuthorizeIpRules workspaces:RevokeIpRules
UpdateWorkspaceBundle	授予更新 WorkSpace 捆绑包中使用的 WorkSpace 图片的权限	写入	workspacebundle* workspaceimage*		
UpdateWorkspaceImagePermission	通过指定其他账户是否有权复制 WorkSpace 图像，授予与其他账户共享或取消共享图像的权限	权限管理	workspaceimage*		
UpdateWorkspacesPool	授予更新 WorkSpaces 池的权限	写入	workspacespoolid*		

Amazon 定义的资源类型 WorkSpaces

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
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}

Amazon 的条件密钥 WorkSpaces

Amazon WorkSpaces 定义了以下条件密钥，这些条件键可用于 IAM 策略的Condition元素中。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据在请求中传递的标签筛选访问	字符串
aws:ResourceTag/${TagKey}	根据与资源关联的标签筛选访问	字符串
aws:TagKeys	根据在请求中传递的标签键筛选访问	ArrayOfString
workspaces:userId	按 WorkSpace 用户的 ID 筛选访问权限	字符串

Amazon X-Ray 的操作、资源和条件键

Amazon X-Ray（服务前缀:`xray`）提供以下特定于服务的资源、操作和条件上下文密钥，供在 IAM 权限策略中使用。

参考：

- 了解如何配置该服务。
- 查看适用于该服务的 API 操作列表。
- 了解如何使用 IAM 权限策略保护该服务及其资源。

主题

- Amazon X-Ray 定义的操作
- Amazon X-Ray 定义的资源类型
- Amazon X-Ray 的条件键

Amazon X-Ray 定义的操作

您可以在 IAM 策略语句的 Action 元素中指定以下操作。可以使用策略授予在 Amazon中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchGetTraceSummaryById[仅权限]	授予权限以检索 ID 指定的跟踪列表的元数据	读取			
BatchGetTraces	授予权限以检索按 ID 指定的跟踪列表。每个跟踪是一组分段文档，由单个请求生成。	列表			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
	GetTraceSummaries 用于获取跟踪列表 IDs				
CancelTraceRetrieval	授予取消 StartTraceRetrieval 使用提供的启动的正在进行的跟踪检索任务的权限 RetrievalToken。成功取消将返回 HTTP 200 响应	读取			
CreateGroup	授予权限以使用名称和筛选条件表达式创建组资源	Write	group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSamplingRule	授予权限以创建规则，用于控制分析的应用程序的采样行为	Write	sampling-rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteGroup	授予权限以删除组资源	写入	group*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	授予权限以删除资源策略	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
DeleteSamplingRule	授予权限以删除采样规则	写入	sampling-rule*		
				aws:ResourceTag/${TagKey}	
GetDistinctTraceGraphs[仅权限]	授予检索一条或多条特定跟踪的不同服务图表的权限 IDs	读取			
GetEncryptionConfig	授予权限以检索 X-Ray 数据的当前加密配置	Read			
GetGroup	授予权限以检索组资源详细信息	Read	group*		
				aws:ResourceTag/${TagKey}	
GetGroups	授予权限以检索所有活动组详细信息	读取			
GetIndexingRules	授予检索所有索引规则的权限。索引规则用于确定通过 CloudWatchLogs 目标采集并由 X-Ray 索引的跨度的服务器端采样率	读取			
GetInsight	授予权限以检索特定见解的详细信息	Read			
GetInsightEvents	授予权限以检索特定见解的事件	Read			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetInsightImpactGraph	授予权限以检索服务图中受特定见解影响的部分	Read			
GetInsightSummaries	授予权限以使用可选筛选器，按照组和时间范围检索所有见解的摘要	读取			
GetRetrievedTracesGraph	授予权限以检索基于事务搜索 CloudWatch 日志组 RetrievalToken 中指定的跟踪的服务图表	读取			
GetSamplingRules	授予权限以检索所有采样规则	Read			
GetSamplingStatisticSummaries	授予权限以检索有关所有采样规则的最新采样结果的信息	Read			
GetSamplingTargets	授予权限以请求服务用于采样请求的规则的采样配额	Read			
GetServiceGraph	授予权限以检索文档，其中包含处理传入请求的服务，以及这些请求作为结果调用的下游服务的介绍	Read			
GetTimeSeriesServiceStatistics	授予权限以获取按时间间隔划分的特定时间范围定义的服务统计数据的聚合	读取			
GetTraceGraph	授予检索一条或多条特定跟踪的服务图表的权限 IDs	读取			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
GetTraceSegmentDestination	授予权限以检索发送到 PutTraceSegments 和 OpenTelemetry API 的数据的当前目的地	读取			
GetTraceSummaries	使用可选筛选器授予在指定时间范围内检索可用跟踪的权限 IDs 和元数据。要获取完整的轨迹，请将轨迹 IDs 传递给 BatchGetTraces	读取			
Link[仅权限]	授予权限以与监视帐户共享 X 射线资源	写入			
ListResourcePolicies	授予权限以列出资源策略	列表			
ListRetrievedTraces	授予 RetrievalToken 从事务搜索 CloudWatch 日志组中检索给定跟踪列表的权限	列表			
ListTagsForResource	授予权限以列出 X-Ray 资源的标签	List	group		
			sampling-rule		
PutEncryptionConfig	授予权限以更新 X-Ray 数据加密配置	权限管理			
PutResourcePolicy	授予权限以创建或更新资源策略	写入			
PutSpans	授予将 OpenTelemetry 跨度上传到 X-Ray 的 Amazon 权限	写入			

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
PutSpansForIndexing[仅权限]	授予将跨度上传到 Amazon X-Ray 以进行索引的权限	写入			
PutTelemetryRecords	授予向服务发送 Amazon X-Ray 守护程序遥测数据的权限	写入			
PutTraceSegments	授予将区段文档上传到 Amazon X-Ray 的权限。X-Ray 开发工具包生成分段文档并发送给 X-Ray 守护程序，再由守护程序批量上传	写入			
StartTraceRetrieval	授予使用指定时间范围启动跟踪检索过程的权限，并在事务搜索 CloudWatch 日志组 IDs 上为给定跟踪启动跟踪检索过程	读取			
TagResource	授予权限以将标签添加到 X-Ray 资源中	Tagging	group		
			sampling-rule		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	授予权限以从 X-Ray 资源中删除标签	Tagging	group		
			sampling-rule		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:TagKeys	
UpdateGroup	授予权限以更新组资源	写入	group*		
				aws:ResourceTag/${TagKey}	
UpdateIndexingRule	授予修改索引规则配置的权限	写入			
UpdateSamplingRule	授予权限以修改采样规则的配置	写入	sampling-rule*		
				aws:ResourceTag/${TagKey}	
UpdateTraceSegmentDestination	授予修改发送到 PutTraceSegments 和 OpenTelemetry API 的数据目的地的权限	写入			

Amazon X-Ray 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
group	`arn:${Partition}:xray:${Region}:${Account}:group/${GroupName}/${Id}`	aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
sampling-rule	arn:${Partition}:xray:${Region}:${Account}:sampling-rule/${SamplingRuleName}	aws:ResourceTag/${TagKey}

Amazon X-Ray 的条件键

Amazon X-Ray 定义了以下可在 IAM 策略Condition元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中传递的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中传递的标签键筛选访问权限	ArrayOfString

相关资源

有关 IAM 用户指南 中的相关信息，请参阅以下资源：

- 教程：创建和附加您的第一个客户托管策略
- Amazon 与 IAM 配合使用的服务
- 策略评估逻辑

用于编程访问的简化 Amazon Web Services 服务 信息

Amazon 以 JSON 格式提供服务参考信息，以简化策略管理工作流程的自动化。借助服务参考信息，您可以通过机器可读文件访问可用的操作、资源和条件密钥。 Amazon Web Services 服务 安全管理员可以建立防护栏，开发人员可以通过识别每个应用程序的可用操作、资源和条件密钥来确保对应用程序的适当访问。 Amazon Web Services 服务 Amazon 提供了的服务参考信息 Amazon Web Services 服务 ，使您可以将元数据整合到策略管理工作流程中。

有关在 IAM 策略中使用的操作、资源和条件密钥的清单，请参阅服务授权参考页面 Amazon Web Services 服务。

共享服务前缀的服务的操作、资源和条件密钥可以在《服务授权参考》中分为多个页面。

> **Note**
>
> 对服务参考信息的更改最长可能需要 24 小时才能反映在服务的元数据列表中。

访问 Amazon Web Services 服务 参考信息

1. 导航到服务参考信息以访问可 Amazon Web Services 服务 用的参考信息列表。

   以下示例显示了服务的部分列表及其各自 URLs 的参考信息：

   ```
   [
       {
           "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. 选择一项服务，然后导航到该服务的`url`字段中的服务信息页面，以查看该服务的操作、资源和条件键的列表。

   以下示例显示了 Amazon S3 的部分服务参考信息列表：

```
{
    "Name": "s3",
    "Actions": [
        {
            "Name": "GetObject",
            "ActionConditionKeys": [
                "s3:AccessGrantsInstanceArn",
                "s3:AccessPointNetworkOrigin",
                "s3:DataAccessPointAccount",
                "s3:DataAccessPointArn",
                "s3:ExistingObjectTag/key",
                "s3:ResourceAccount",
                "s3:TlsVersion",
                "s3:authType",
                "s3:if-match",
                "s3:if-none-match",
                "s3:signatureAge",
                "s3:signatureversion",
                "s3:x-amz-content-sha256"
            ],
            "Resources": [
                {
                    "Name": "object"
                }
            ]
        },
        {
            "Name": "ListBucket",
            "ActionConditionKeys": [
                "s3:AccessGrantsInstanceArn",
                "s3:AccessPointNetworkOrigin",
                "s3:DataAccessPointAccount",
                "s3:DataAccessPointArn",
                "s3:ResourceAccount",
                "s3:TlsVersion",
                "s3:authType",
                "s3:delimiter",
                "s3:max-keys",
                "s3:prefix",
                "s3:signatureAge",
                "s3:signatureversion",
                "s3:x-amz-content-sha256"
            ],
```

```
            "Resources": [
                {
                    "Name": "bucket"
                }
            ]
        },
        ...
    ],
    "ConditionKeys": [
        {
            "Name": "s3:TlsVersion",
            "Types": [
                "Numeric"
            ]
        },
        {
            "Name": "s3:authType",
            "Types": [
                "String"
            ]
        },
        ...
    ],
    "Resources": [
        {
            "Name": "accesspoint",
            "ARNFormats": [
                "arn:${Partition}:s3:${Region}:${Account}:accesspoint/
${AccessPointName}"
            ]
        },
        {
            "Name": "bucket",
            "ARNFormats": [
                "arn:${Partition}:s3:::${BucketName}"
            ]
        }
        ...
    ],
    "Version": "v1.1"
}
```

3. 通过服务 URL 下载 JSON 文件以用于您的策略制定工作流程。

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。