aws

用户指南

标记 AWS 资源和标签编辑器

版本 1.0

标记 AWS 资源和标签编辑器: 用户指南

Table of Contents

什么是标签编辑器？

标签编辑器使您能够有效地管理标签。标签是键和值对，用作组织 AWS 资源的元数据。对于大多数 AWS 资源，您可以在创建资源时选择添加标签。资源示例包括亚马逊弹性计算云 (AmazonEC2) 实例、亚马逊简单存储服务 (Amazon S3) Simple Service 存储桶或中的密钥。 AWS Secrets Manager

> **Important**
>
> 请勿在标签中存储个人身份信息 (PII) 或其他机密或敏感信息。我们通过标签为您提供账单和管理服务。标签不适合用于私有或敏感数据。

标签可帮助您管理、识别、组织、搜索和筛选资源。您可以创建标签，按用途、所有者、环境或其他标准对资源进行分类。

每个标签具有两个部分：

- 标签键（例如，`CostCenter`、`Environment` 或 `Project`）。标签键区分大小写。
- 标签值（例如，`111122223333` 或 `Production`）。与标签键一样，标签值区分大小写。

> **Note**
>
> 尽管标签密钥区分大小写，但对IAM资源IAM进行了额外的验证，以防止应用仅大小写不同的标签密钥。我们建议不要使用只有大小写不同的按键。相反，您可以使用服务控制策略 (SCPs)，它可以集中控制组织中IAM用户和IAM角色的最大可用权限。

资源标记方法

有三种方法可以为您的 AWS 资源添加标签：

- AWS 服务 API操作 — 直接支持的标记API操作。 AWS 服务要了解每种功能 AWS 服务 提供的标记功能，请参阅文档索引中的服务AWS 文档。
- 标签编辑器控制台-某些服务支持使用标签编辑器控制台添加标签。
- R@@ esource Groups 标记 API — 大多数服务还支持使用进行标记。AWS Resource Groups Tagging API

> **Note**
>
> 您还可以使用AWS Service Catalog TagOptions 资源库轻松管理预配置产品的标签。A TagOption是在 Service Catalog 中管理的键值对。它不是 AWS 标签，而是用作根据创建 AWS 标签的模板 TagOption。

您可以在 AWS中为所有产生成本的服务标记资源。对于以下服务， AWS 推荐支持标签的新替代方案 AWS 服务 ，以更好地满足客户用例。

Amazon Cloud Directory	亚马逊 CloudSearch	Amazon Cognito Sync
AWS Data Pipeline	Amazon Elastic Transcoder	Amazon Machine Learning
AWS OpsWorks Stacks	Amazon S3 Glacier Direct	Amazon SimpleDB
Amazon WorkSpaces 应用程序管理器	AWS DeepLens	

了解更多

本页提供有关标记 AWS 资源的一般信息。有关在特定 AWS 服务中标记资源的更多信息，请参阅其文档。以下内容也是有关标记的有用信息来源：

- 有关信息 AWS Resource Groups Tagging API，请参阅《Resource Groups 标记API参考指南》。
- 有关各自 AWS 服务 提供的标记功能的信息，请参阅文档索引中的服务AWS 文档。
- 有关在IAM策略中使用标签来帮助控制谁可以查看您的 AWS 资源并与之交互的信息，请参阅IAM用户指南中的使用标签控制IAM用户和角色的访问权限。

最佳实践和策略

这些部分提供有关为 AWS 资源添加标签和使用标签编辑器时的最佳做法和策略的信息。

标记最佳实践

在为 AWS 资源创建标签策略时，请遵循最佳实践：

- 请勿在标签中添加个人身份信息 (PII) 或其他机密或敏感信息。许多 AWS 服务都可以访问标签，包括账单。标签不适合用于私有或敏感数据。
- 对标签使用标准化的区分大小写格式，并跨所有资源类型一致地应用该格式。
- 考虑支持多种用途的标签准则，如管理资源访问控制、成本跟踪、自动化和组织。
- 运用自动化工具帮助您管理资源标签。标签编辑器和 Res ource Groups Taggin g API 支持对标签进行编程控制，从而更轻松地自动管理、搜索和筛选标签和资源。
- 使用过多的标签而不是过少的标签。
- 请记住，更改标签以适应不断变化的业务需求很容易，但要考虑未来更改的后果。例如，更改访问控制标签意味着您还必须更新引用这些标签并控制对资源的访问的策略。
- 您可以通过使用 AWS Organizations创建和部署标签策略，自动强制执行贵组织选择采用的标记标准。标签策略使您能够指定标记规则，这些规则可以定义有效密钥名称和对每个密钥有效的值。您可以选择仅监控，从而使您有机会评估和清理现有标签。一旦您的标签符合您选择的标准，您就可以在标签策略中启用强制执行，以防止创建不合规的标签。有关更多信息，请参阅《AWS Organizations 用户指南》中的标签策略。

标签命名最佳实践

以下是我们建议您在使用标签时运用的最佳实践和命名约定。

AWS 标签的密钥名称区分大小写，因此请确保使用一致性。例如，标签密钥 `CostCenter` 和 `costcenter` 是不同的。其中一个标签密钥可能会被配置为成本分配标签，用于财务分析和报告，而另一个标签密钥则可能没有被配置为相同用途。

许多标签是由各种人预定义 AWS 或自动创建的 AWS 服务。很多AWS 生成标签的密钥名称全部使用小写字母，名称中的单词之间用连字符分隔，使用后跟冒号的前缀来标识标签的源服务。例如，请参阅以下文档：

- `aws:ec2spot:fleet-request-id`是一个标识启动该实例的 Amazon EC2 竞价型实例请求的标签。
- `aws:cloudformation:stack-name` 是标签，用于标识创建资源的 AWS CloudFormation 堆栈。
- `elasticbeanstalk:environment-name` 是标签，用于标识创建资源的应用程序。

考虑使用以下规则命名您的标签：

- 单词全部小写。
- 使用连字符分隔单词。

- 使用后跟冒号的前缀来标识组织名称或缩写名称。

例如，对于名为的虚构公司 AnyCompany，您可以定义如下标签：

- anycompany:cost-center 标识内部成本中心代码。
- anycompany:environment-type 确定环境是开发、测试还是生产环境。
- anycompany:application-id 标识为其创建资源的应用程序。

前缀可确保标签可以按照您的组织定义清晰识别，而不是由 AWS 您可能使用的第三方工具进行识别。使用所有小写字母和连字符作为分隔符，可以避免对如何大写标签名称产生混淆。例如，anycompany:project-id 比 ANYCOMPANY:ProjectID、anycompany:projectID 或 Anycompany:ProjectId 更易记。

标签命名限制和要求

标签应遵循以下基本命名和使用要求：

- 每个资源最多可以有 50 个用户创建的标签。
- 以 aws: 开头的系统创建标签将保留供 AWS 使用，并且不计入此限制。您无法编辑或删除以 aws: 前缀开头的标签。
- 对于每个资源，每个标签键都必须是唯一的，每个标签键只能有一个值。
- 标签密钥必须至少为 1，在 UTF -8 中最多包含 128 个 Unicode 字符。
- 标签值必须最小为 0，在 UTF -8 中最多为 256 个 Unicode 字符。
- 允许的字符可能因 AWS 服务而异。有关您可以使用哪些字符来标记特定 AWS 服务中的资源的信息，请参阅其文档。通常，允许使用的字符是字母、数字、可用 UTF -8 表示的空格以及以下字符：_.:/= +-@。
- 标签键和值区分大小写。最佳实践是，决定利用标签的策略并在所有资源类型中一致地实施该策略。例如，决定是使用 Costcenter、costcenter 还是 CostCenter，以及是否对所有标签使用相同的约定。避免将类似的标签用于不一致的案例处理。

常见标签策略

可以使用以下标记策略帮助识别和管理 AWS 资源。

内容

- 资源整理标签
- 成本分配标签
- 自动化标签
- 访问控制标签
- 标签监管

资源整理标签

标签是在中组织 AWS 资源的好方法 AWS Management Console。您可以配置标签来与资源一起显示，并且可以按标签进行搜索和筛选。使用该 AWS Resource Groups 服务，您可以基于一个或多个标签或部分标签创建 AWS 资源组。您也可以根据群组在 AWS CloudFormation 堆栈中的出现情况来创建群组。使用 Resource Groups 和标签编辑器，您可以在一个位置整合和查看由多个服务、资源和区域组成的应用程序的数据。

成本分配标签

AWS Cost Explorer 和详细的账单报告可让您按标签细分 AWS 成本。通常，您可以使用诸如成本中心/业务部门、客户或项目之类的业务标签将 AWS 成本与传统的成本分配维度相关联。但是，成本分配报告中可以包含任何标签。这使您可以将成本与技术或安全维度（例如特定应用程序、环境或合规性项目）关联起来。

对于某些服务，您可以使用 AWS生成的`createdBy`标签进行成本分配，以帮助考虑原本可能未分类的资源。`createdBy` 标签仅适用于受支持的 AWS 服务和资源。它的值包含与特定事件API或控制台事件相关的数据。有关更多信息，请参阅《AWS Billing and Cost Management 用户指南》中的 AWS生成的成本分配标签。

自动化标签

资源或特定于服务的标签通常用于在自动化活动期间筛选资源。自动化标签用于选择加入或退出自动化任务，或识别要存档、更新或删除的资源的特定版本。例如，您可以运行自动 `start` 或 `stop` 脚本，这些脚本可在非工作时间内关闭开发环境以降低成本。在这种情况下，Amazon Elastic Compute Cloud (AmazonEC2) 实例标签是识别要退出此操作的实例的简单方法。对于查找和删除陈旧或滚动的 Amazon EBS 快照的脚本，快照标签可以增加搜索条件的额外维度。 out-of-date

访问控制标签

IAM策略支持基于标签的条件，允许您根据特定标签或标签值限制IAM权限。例如，IAM用户或角色权限可以包括根据标签限制对特定环境（例如开发、测试或生产）的EC2API调用的条件。同样的策略

可用于限制对特定亚马逊虚拟私有云 (AmazonVPC) 网络的API调用。对基于标签的资源级IAM权限的 Support 因服务而异。使用基于标签的条件进行访问控制时，请务必定义和限制谁可以修改标签。有关使用标签控制 AWS 资源API访问权限的更多信息，请参阅《IAM用户指南》IAM中与之配合使用的 AWS 服务。

标签监管

有效的标记策略使用标准化标签，并以编程方式在资源之间 AWS 以一致的方式应用这些标签。您可以使用被动和主动方法来管理 AWS 环境中的标签。

- 被动治理用于使用诸如资源组（Resource Groups Taggin API g）和自定义脚本之类的工具查找未正确标记的资源。 AWS Config 规则要手动查找资源，您可以使用标签编辑器和详细账单报告。
- 主动式治理使用诸如 AWS CloudFormation Service Catalog AWS Organizations、中的标签策略或IAM资源级权限之类的工具来确保在创建资源时一致地应用标准化标签。

  例如，您可以使用 AWS CloudFormation `Resource Tags`属性将标签应用于资源类型。在服务目录中，您可以添加在产品启动时自动组合和应用于产品的产品组合和产品标签。更严格的主动监管形式包括自动化任务。例如，您可以使用 Resource Groups 标记API来搜索 AWS 环境的标签，或者运行脚本来隔离或删除标记不当的资源。

为类别添加标签

最有效地使用标签的公司通常会创建与业务相关的标签分组，以便按照技术、业务和安全维度整理其资源。使用自动化流程管理其基础设施的公司还包括其他特定于自动化的标签。

技术标签	自动化标签	企业标签	安全标签
• 名称 – 标识各项资源 • 应用程序 ID – 标识与特定应用程序相关的资源 • 应用程序角色 – 描述特定资源（如 Web 服务器、消息代理、数据库）的功能	• 日期/时间 – 标识应启动、停止、删除或轮换资源的日期或时间 • 选择进入/选择退出 – 指示资源是否应包含在自动化活动中，例如启动、停止或调整实例大小	• 项目 – 标识资源支持的项目 • 所有者 – 标识谁负责资源 • 成本中心/业务单位 – 标识与资源关联的成本中心或业务单位，通常用于成本分配和跟踪	• 机密性 – 资源支持的特定数据机密性级别的标识符。 • 合规性 – 必须遵守特定合规性要求的工作负载的标识符

技术标签	自动化标签	企业标签	安全标签
• 群集 – 标识共享通用配置并为应用程序执行特定功能的资源群 • 环境 – 区分开发资源、测试资源和生产资源 • 版本 – 帮助区分资源或应用程序的版本	• 安全 — 确定要求，例如加密或启用 Amazon VPC 流日志；确定需要额外审查的路由表或安全组	• 客户 – 标识由特定的资源组提供服务的特定客户端	

开始使用标签编辑器

> **Important**
>
> 请勿在标签中存储个人身份信息 (PII) 或其他机密或敏感信息。我们通过标签为您提供账单和管理服务。标签不适合用于私有或敏感数据。

请使用标签编辑器，以同时为多个资源添加、编辑或删除标签。通过使用标签编辑器，您可以搜索要标记的资源，然后在搜索结果中管理这些资源的标签。

要启动标签编辑器

1. 登录 。AWS Management Console.
2. 执行下列步骤之一：
   - 选择 服务。然后，在管理和治理下，选择资源组和标签编辑器。在左侧的导航窗格中，选择 标签编辑器。
   - 使用直接链接：AWS 标签编辑器控制台。

标签并非适用于所有资源。有关标签编辑器支持哪些资源的信息，请参阅中支持的资源类型中的标签编辑器标记列 AWS Resource Groups 用户指南。如果不支持您要标记的资源类型，请让 AWS 通过选择控制台窗口左下角的 “反馈” 来了解。

有关标记资源所需的权限和角色的信息，请参阅设置权限。

主题

使用标签编辑器的先决条件

在开始为资源添加标签之前，请确保您的资源处于活动状态 AWS 账户 拥有现有资源以及标记资源和创建群组的适当权限。

主题

- 注册获取 AWS 账户
- 创建具有管理访问权限的用户
- 创建资源

注册获取 AWS 账户

如果你没有 AWS 账户，请完成以下步骤来创建一个。

报名参加 AWS 账户

1. 打开https://portal.aws.amazon.com/billing/注册。
2. 按照屏幕上的说明进行操作。

   在注册时，将接到一通电话，要求使用电话键盘输入一个验证码。

   当你注册时 AWS 账户，一个 AWS 账户根用户已创建。root 用户可以访问所有内容 AWS 服务 以及账户中的资源。作为安全最佳实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

AWS 注册过程完成后会向您发送一封确认电子邮件。您可以随时前往 https://aws.amazon.com/并选择“我的账户”，查看您当前的账户活动并管理您的账户。

创建具有管理访问权限的用户

在你注册之后 AWS 账户，保护你的 AWS 账户根用户，启用 AWS IAM Identity Center，然后创建一个管理用户，这样你就不会使用 root 用户来执行日常任务。

保护你的 AWS 账户根用户

1. 登录 。AWS Management Console以账户所有者的身份选择 Root 用户并输入你的 AWS 账户 电子邮件地址。在下一页上，输入您的密码。

   有关使用 root 用户登录的帮助，请参阅中以 root 用户身份登录 AWS 登录 用户指南。
2. 为您的 root 用户开启多重身份验证 (MFA)。

   有关说明，请参阅为您的MFA设备启用虚拟设备 AWS 账户 用户指南中的 root IAM 用户（控制台）。

创建具有管理访问权限的用户

1. 启用 “IAM身份中心”。

   有关说明，请参阅启用 AWS IAM Identity Center中的 AWS IAM Identity Center 用户指南。
2. 在 IAM Identity Center 中，向用户授予管理访问权限。

   有关使用教程 IAM Identity Center 目录 作为您的身份来源，请参阅使用默认设置配置用户访问权限 IAM Identity Center 目录中的 AWS IAM Identity Center 用户指南。

以具有管理访问权限的用户身份登录

- 要使用您的 Ident IAM ity Center 用户登录URL，请使用您在创建 Ident IAM ity Center 用户时发送到您的电子邮件地址的登录信息。

  有关使用 Ident IAM ity Center 用户登录的帮助，请参阅登录 AWS 访问中的门户 AWS 登录 用户指南。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个遵循应用最低权限权限的最佳实践的权限集。

   有关说明，请参阅中的创建权限集 AWS IAM Identity Center 用户指南。
2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

   有关说明，请参阅中的添加群组 AWS IAM Identity Center 用户指南。

创建资源

你的里面必须有资源 AWS 账户 要标记。有关支持的资源类型的更多信息，请参阅《支持的资源类型》下的 “标签编辑器标记” 列 AWS Resource Groups 用户指南。

设置权限

要充分利用标签编辑器，您可能需要更多权限来标记资源或查看资源的标签密钥和值。这些权限分为以下类别：

- 面向单个服务的权限，用于标记和在资源组中包含相应服务的资源。

- 使用标签编辑器控制台所需的权限。

如果您是管理员，则可以通过创建策略来为用户提供权限 AWS Identity and Access Management (IAM) 服务。您首先创建IAM角色、用户或群组，然后应用具有所需权限的策略。有关创建和附加IAM策略的信息，请参阅使用策略。

面向单个服务的权限

> **Important**
>
> 本节介绍如果要标记其他资源的资源，则需要哪些权限 AWS 服务控制台和APIs。

要向资源添加标签，您需要拥有对资源所属的服务的必要权限。例如，要标记亚马逊EC2实例，您必须拥有在该服务（例如 Amazon）中执行标记操作的API权限 EC2 CreateTags操作。

使用标签编辑器控制台所需的权限

要使用标签编辑器控制台列出和标记资源，必须在中的用户政策声明中添加以下权限IAM。你可以添加任一项 AWS 由以下人员维护和保持更新的托管策略 AWS，或者您可以创建和维护自己的自定义策略。

使用 AWS 标签编辑器权限的托管策略

标签编辑器支持以下内容 AWS 托管策略，您可以使用这些策略向用户提供一组预定义的权限。正如您创建的任何其他策略一样，您可以将这些托管策略附加到任何角色、用户或组。

ResourceGroupsandTagEditorReadOnlyAccess

此策略向附加的IAM角色或用户授予对两个角色或用户调用只读操作的权限 AWS Resource Groups 和标签编辑器。要读取资源的标签，您还必须通过单独的策略拥有该资源的权限。请在以下重要说明中了解更多信息。

ResourceGroupsandTagEditorFullAccess

此策略向附加的IAM角色或用户授予在标签编辑器中调用任何 Resource Groups 操作以及读取和写入标签操作的权限。要读取或写入资源的标签，您还必须通过单独的策略拥有该资源的权限。请在以下重要说明中了解更多信息。

Important

前两项策略授予调用标签编辑器操作和使用标签编辑器控制台的权限。但是，您不仅需要拥有调用该操作的权限，还必须拥有您尝试访问其标签的特定资源的相应权限。要授予对标签的访问权限，您还必须附加以下策略之一：

- 这些区域有： AWS 托管策略 ReadOnlyAccess授予每项服务资源的只读操作权限。 AWS 自动使本政策与新政策保持同步 AWS 服务 当它们可用时。
- 许多服务都提供特定于服务的只读服务 AWS 托管策略，您可以使用这些策略来限制仅访问该服务提供的资源。例如，亚马逊EC2提供 AmazonEC2ReadOnlyAccess.
- 您可以创建自己的策略，仅授予您希望用户访问的少数服务和资源的特定只读操作的权限。此策略使用允许列表或拒绝列表策略。

  允许列表策略利用了这样一个事实：在策略中，在明确允许访问之前，默认情况下访问是被拒绝的。因此，您可以使用以下示例中体现出的政策。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [ "tag:*" ],
            "Resource": "<ARNs of resources to allow tagging>"
        }
    ]
}
```

或者，您可以使用拒绝列表策略，允许访问除您明确屏蔽的资源之外的其他资源。这需要一个针对相关用户允许访问的单独策略。然后，以下示例策略拒绝访问由 Amazon 资源名称 (ARN) 列出的特定资源。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
             "Action": [ "tag:*" ],
            "Resource": "<ARNs of resources to disallow tagging>"
        }
    ]
```

```
}
```

手动添加标签编辑器权限

- `tag:*`（此权限允许所有标签编辑器操作。如果您想限制用户的可用操作，则可以将星号替换为特定操作或替换为以逗号分隔的操作列表。）
- `tag:GetResources`
- `tag:TagResources`
- `tag:UntagResources`
- `tag:getTagKeys`
- `tag:getTagValues`
- `resource-explorer:*`
- `resource-groups:SearchResources`
- `resource-groups:ListResourceTypes`

> **Note**
>
> 该`resource-groups:SearchResources`权限允许标签编辑器在您使用标签键或值筛选搜索时列出资源。
> 该`resource-explorer:ListResources`权限允许标签编辑器在您搜索资源时列出资源，而无需定义搜索标签。

授予使用标签编辑器的权限

添加策略以供使用 AWS Resource Groups 然后将标签编辑器设置为角色，请执行以下操作。

1. 打开IAM控制台进入角色页面。
2. 找到要授予其标签编辑器权限的角色。选择新角色以打开该角色的摘要页面。
3. 在权限选项卡中，请选择添加权限。
4. 选择直接附加现有策略。
5. 选择创建策略。

6. 在JSON选项卡上，粘贴以下政策声明。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-explorer:*",
        "resource-groups:SearchResources",
        "resource-groups:ListResourceTypes"
      ],
      "Resource": "*"
    }
  ]
}
```

> **Note**
>
> 该策略声明仅授予执行标签编辑器操作的权限。

7. 依次选择 Next: Tags（下一步：标签）和 Next: Review（下一步：查看）。
8. 输入新策略的名称和说明。例如，**`AWSTaggingAccess`**。
9. 选择创建策略。

现在，策略已保存在中IAM，您可以将其附加到其他委托人，例如角色、群组或用户。有关如何向委托人添加策略的更多信息，请参阅IAM用户指南中的添加和删除IAM身份权限。

基于标签的授权和访问控制

AWS 服务 支持以下内容：

- 基于操作的策略 – 例如，您可以创建一个策略，以允许用户执行 `GetTagKeys` 或 `GetTagValues` 操作，但不能执行其他操作。
- 策略中的资源级权限 — 许多服务支持使用ARNs在策略中指定单个资源。

- 根据标签进行授权 – 很多服务支持在策略的条件中使用资源标签。例如，您可以创建一个策略，以允许用户对跟用户拥有相同标签的组具有完全访问权限。有关更多信息，请参阅用ABAC途 AWS？在 AWS Identity and Access Management 用户指南。
- 临时凭证 – 用户可以通过允许标签编辑器操作的策略担任角色。

标签编辑器不使用服务相关角色。

有关标签编辑器如何与之集成的更多信息 AWS Identity and Access Management (IAM)，请参阅中的以下主题 AWS Identity and Access Management 用户指南：

- AWS 与之配合使用的服务 IAM
- 标签编辑器的操作、资源和条件密钥
- 控制对的访问权限 AWS 使用策略的资源

查找要标记的资源

使用标签编辑器，您可以构建查询，在一个或多个中查找可用于标记 AWS 区域 的资源。您可以选择最多 20 种单独的资源类型，或根据所有资源类型构建查询。您的查询可以包含已具有标签的资源，也可以包含没有标签的资源。有关更多信息，请参阅 AWS Resource Groups 用户指南中支持的资源类型中的标签编辑器标记列。

在找到要标记的资源后，您可以使用标签编辑器添加标签，或者查看、编辑或删除标签。

查找要标记的资源

1. 打开标签编辑器控制台。
2. （可选）选择要 AWS 区域 在其中搜索要标记的资源。默认情况下，将使用您的当前区域。对于本程序，请选择 us-east-1 和 us-west-2。
3. 从资源类型下拉列表中，选择至少一种资源类型。您可以一次为最多 20 种单独的资源类型添加或编辑标签，或者选择所有资源类型。对于此过程，请选择AWS::: Instance 和EC2:: S3AWS:: Bucket。
4. （可选）在标签字段中，输入一个标签密钥或标签密钥和值对，以将当前 AWS 区域 区域中的资源限制为仅使用指定值标记的资源。输入标签密钥时，列表中会显示当前区域中匹配的标签密钥。您可以从列表中选择标签密钥。在键入足够多的字符以与现有键匹配时，标签编辑器将自动完成标签键。在完成您的标签时，请选择 Add (添加) 或按 Enter。在该示例中，筛选具有 Stage 标签键的资源。标签值是可选的，但会进一步缩小查询的结果。要添加更多标签，请选择添加。查询将 AND 运算符分配给标签，以便查询只返回与指定的资源类型和所有指定的标签匹配的资源。

   > **Note**
   >
   > 标签编辑器控制台目前不支持通配符。

   要查找具有某个标签键的多个值的资源，请将另一个具有相同键的标签添加到查询中，但指定不同的值。这些结果包括使用相同标签键标记并具有任何选定值的所有资源。搜索区分大小写。

   将标签框保留空白，以在所选 AWS 区域中查找具有指定类型的所有资源。该查询返回具有任何标签的资源，并包括没有标签的资源。要从查询中删除某个标签，请在其标签上选择 X。

   要查找带有标签但值为空的资源，请选择（空值）。

> **Note**
>
> 在查找具有指定标签的资源之前，必须将这些标签应用于当前 AWS 区域中至少一个具有指定类型的资源。

5. 在查询准备就绪时，请选择搜索资源。结果将在资源搜索结果区域中显示为表格。

   要筛选大量资源，请在筛选资源中输入任何筛选文本，例如，资源名称的一部分。

   > **Note**
   >
   > 您可以使用子字符串来筛选结果。

6. （可选）要配置标签编辑器在资源搜索结果中显示的列，请在资源搜索结果中选择首选项齿轮图标。

   在首选项页面上，选择要在搜索结果中显示的行数。如果您想查看表格中的所有文本，请选中换行复选框。

   启用您希望标签编辑器在结果中显示的列。您可以显示在搜索结果中出现的每个标签密钥的列或选定的一部分搜索结果。在找到要标记的资源后，您可以随时执行该操作。要启用某列，请选择标签旁边的切换图标，然后将其从关闭 更改为开启 。

   在配置完可见的列和显示的行数后，请选择确认。

查看和编辑所选资源的现有标签

标签编辑器显示位于查找要添加标签的资源查询结果中的选定资源上的现有标签。

如果您按照上一节所述启用了任何标签列，可在搜索结果中看到每个资源的该标签的当前值。

> **Note**
>
> 本主题说明如何编辑单个资源的标签。您还可以同时批量编辑多个选定资源的标签。有关更多信息，请参阅 使用标签编辑器管理标签。

在搜索结果表中编辑内联标签

1. 选择您想要对其进行编辑的资源上的标签的值。

> **Note**
>
> - 如果当前所选资源不带有所选密钥的标签，则该值将显示为（未标记）。
> - 如果所选资源的确有带有所选密钥的标签，但没有值，则该值将显示为“–”。

2. 您可以输入新值，或从其他带有该标签的资源上已有的值中任意选择。您也可以选择移除标签，从该资源中删除标签。

查阅单个资源的所有标签

1. 在 查找要标记的资源 查询结果中，在 标签 列中为要查看现有标签的任何资源选择一个数字。在 Tags (标签) 列中包含短划线的资源没有现有的标签。
2. 在资源标签中查看现有的标签。在管理标签页面更改或移除标签时，您还可以通过选择管理所选资源的标签来打开此窗口。

> **Note**
>
> 如果您没有看到最近应用于资源的标签，请尝试刷新浏览器窗口。

将结果导出为 .csv 文件

您可以将查找要添加标签的资源查询结果导出为以逗号分隔的值 (.csv) 文件。.csv 文件包括资源名称、服务、区域、资源IDs、标签总数以及集合中每个唯一标签键对应的一列。.csv 文件可以帮助您为组织中的资源制订标记策略，或者确定资源之间的标记重叠或不一致问题。

1. 在 “查找要标记的资源” 查询的结果中，选择 “将资源导出到” CSV。
2. 在浏览器提示您时，选择打开 .csv 文件，或将其保存到方便的位置。

使用标签编辑器管理标签

在找到要标记的资源后，您可以添加、删除和编辑部分或全部搜索结果的标签。标签编辑器显示附加到资源的所有标签。它还会显示这些标签是在标签编辑器中添加的、由资源的服务控制台添加的，还是通过使用添加的API。

> **Important**
>
> 请勿在标签中存储个人身份信息 (PII) 或其他机密或敏感信息。我们通过标签为您提供账单和管理服务。标签不适合用于私有或敏感数据。

> **管理标签的其他方法**
>
> 本主题讨论如何使用标签编辑器为资源添加标签 AWS Management Console。 但是，您也可以管理自己的标签 AWS 使用以下工具获得资源：
>
> - 您可以在 shell 提示符下键入命令或编写脚本`resourcegroupstaggingapi`命令，方法是使用中的命令 AWS Command Line Interface (AWS CLI).
> - 你可以创建并运行 PowerShell 使用脚本 AWS Resource Groups 在里面API加标签 AWS Tools for PowerShell Core.
> - 您可以使用任何可用的程序来创建和运行程序 AWS SDKs通过使用资源组标记 APIs，例如APIsPython 的标记或 Jav a 的标记APIs。

在添加、删除或编辑现有标签时，您仅在查找要添加标签的资源查询结果中选择的资源上更改标签。您最多可以选择 500 个要在其中管理标签的资源。

将标签添加到选定的资源

您可以使用标签编辑器将标签添加到位于查找要添加标签的资源查询结果中的选定资源。

> **Note**
>
> 本主题描述如何批量编辑多个资源的标签。您也可以编辑单个资源的标签值。有关更多信息，请参阅 查看和编辑所选资源的现有标签。

1. 打开标签编辑器控制台，然后提交一个查询，以返回您要标记的多个资源。
2. 在查找要添加标签的资源查询结果表格中，选中要添加标签的资源旁边的复选框。在表格上部的筛选资源中输入一个文本字符串，以筛选资源的名称、ID、标签键或标签值的一部分。在标签列中，请注意结果中的资源已应用标签。
3. 选中一个或多个资源的复选框，然后选择管理所选资源的标签。
4. 在管理标签页面上，查看选择的资源上的标签。虽然原始查询返回了更多资源，您仅将标签添加到在步骤 1 中选择的那些资源。选择 Add tag（添加标签）。
5. 输入一个标签键和可选的标签值。在此过程中，您将添加标签密钥 **`Team`** 和标签值 **`Development`**。

   > **Note**
   >
   > 资源最多可以包含 50 个用户应用的标签。如果用户应用的标签接近 50 个，则可能无法向资源添加新标签。 AWS 生成的标签不适用于 50 个标签的限制。标签键还必须在选定资源中是唯一的。您无法添加密钥与已经存在于选定资源中的标签密钥匹配的新标签。

6. 在添加完标签后，请选择查看并应用更改。
7. 如果您接受这些更改，请选择将更改应用于所有选定的标签。
8. 根据您选择的资源数量，应用新标签可能需要几分钟的时间。不要离开页面或在同一浏览器选项卡中打开不同的页面。如果更改成功，则会在页面顶部显示绿色成功横幅。等待在页面上显示成功或失败横幅，然后再继续。

   如果对部分或全部资源的标签更改失败，请参阅对标签更改进行故障排除。在解决标签更改失败问题（例如，权限不足）后，您可以在标签更改失败的资源上重试标签更改。有关更多信息，请参阅 the section called “重试失败的标签更改”。

编辑选定资源的标签

您可以使用标签编辑器更改位于查找要添加标签的资源查询结果中的选定资源上的现有标签值。如果编辑某个标签，将会更改具有相同标签键的所有选定资源上的标签值。您无法对标签密钥重命名，但可以删除标签并创建新标签以替换最初的标签密钥。这会删除选定资源上具有该键的所有标签。

> **Important**
>
> 请勿在标签中存储个人身份信息 (PII) 或其他机密或敏感信息。我们通过标签为您提供账单和管理服务。标签不适合用于私有或敏感数据。

1. 在查找要添加标签的资源查询结果中，选中要更改现有标签的资源旁边的复选框。在筛选资源中输入一个文本字符串，以筛选资源的名称或 ID 的一部分。在标签列中，请注意结果中的资源已应用标签。
2. 选择管理选定资源的标签。
3. 在管理标签页面上的编辑选定资源的标签中，查看选定的资源上的标签。虽然原始查询返回了更多资源，您仅更改在步骤 1 中选择的那些资源上的标签。
4. 更改、添加或删除标签值。现有标签必须具有标签键，但标签值是可选的。

   在本程序中，我们将 **Team** 标签值更改为 **QA**。

   如果选定资源中的同一密钥具有不同的值，则会在标签值字段中显示选定的资源具有不同的标签值。在这种情况下，将光标放在框中将打开一个下拉列表，其中列出选定资源中的该标签键的所有可用值。

   如果选定的资源具有所需的标签值，则会在键入时突出显示该标签值。例如，如果选定的资源已具有标签值 **QA**，则会在键入 **Q** 时突出显示该值。下拉列表中的值有助于将标签值在资源之间保持一致。将在所有选定的资源上更改标签值。在该示例中，对于具有 **Team** 标签键的所有选定资源，标签值将更改为 **QA**。对于没有 **Team** 标签的选定资源，将添加具有 **QA** 值的 **Team** 标签。
5. 在更改完标签后，请选择查看并应用更改。
6. 如果您接受这些更改，请选择将更改应用于所有选定的标签。
7. 根据您选择的资源数量，编辑标签可能需要几分钟的时间。不要离开页面或在同一浏览器选项卡中打开不同的页面。如果更改成功，则会在页面顶部显示绿色成功横幅。等待在页面上显示成功或失败横幅，然后再继续。

   如果对部分或全部资源的标签更改失败，请参阅对标签更改进行故障排除。在解决标签更改失败的根本原因（例如，权限不足）后，您可以在标签更改失败的资源上重试标签更改。有关更多信息，请参阅 the section called “重试失败的标签更改”。

从选定的资源中删除标签

您可以使用标签编辑器从位于查找要添加标签的资源查询结果上的选定资源中删除标签。如果删除某个标签，则会从具有该标签的所有选定资源中删除该标签。由于您无法编辑标签密钥，因此，如果需要编辑标密钥，您可以删除标签并将其替换为新标签。这会删除选定资源上具有该键的所有标签。

1. 在查找要添加标签的资源查询结果中，选中要从中删除标签的资源旁边的复选框。在筛选资源中输入一个文本字符串，以筛选资源的名称或 ID 的一部分。
2. 选择管理选定资源的标签。
3. 在管理标签页面上的编辑选定资源的标签中，查看选择的资源上的标签。虽然原始查询返回了更多资源，您仅更改在步骤 1 中选择的那些资源上的标签。
4. 选中要删除的任何标签旁边的删除标签。在此程序中，我们删除了 **Team** 标签。

   > **Note**
   >
   > 如果选择删除标签，则会从具有某个标签的所有选定资源中删除该标签。

5. 选择查看并应用更改。
6. 在确认页面上，选择将更改应用于所有选定的标签。
7. 根据您选择的资源数量，删除标签可能需要几分钟的时间。不要离开页面或在同一浏览器选项卡中打开不同的页面。如果更改成功，则会在页面顶部显示绿色成功横幅。等待在页面上显示成功或失败横幅，然后再继续。

   如果对部分或全部资源的标签更改失败，请参阅对标签更改进行故障排除。在解决标签更改失败的根本原因（例如，权限不足）后，您可以在标签更改失败的资源上重试标签更改。有关更多信息，请参阅 the section called “重试失败的标签更改”。

在IAM权限策略中使用标签

AWS Identity and Access Management (IAM) 是您 AWS 服务 用来创建和管理权限策略，用于确定谁可以访问您的 AWS 资源。每次访问 AWS 服务或读取或写入 AWS 资源的尝试都受到IAM策略的控制。

这些策略允许您对资源进行精细访问。您可以使用其中的特征微调此访问权限，即策略的 `Condition` 元素。可通过该元素指定必须与请求匹配的条件，以确定请求是否可以继续。您可以使用 `Condition` 元素检查以下内容：

- 附加到发出请求的用户或角色的标签。
- 附加到作为请求对象的资源上的标签。

标签和基于属性的访问控制

标签可能是您的 AWS 访问控制策略的重要组成部分。有关在基于属性的访问控制 (ABAC) 策略中使用标签作为属性的信息，请参阅《用户指南》中的 “使用标签控制对 AWS 资源的访问” 和 “使用标签控制IAM用户和角色的访问权限” IAM。

教程：根据AWS Identity and Access Management 用户指南中的标签定义访问 AWS 资源的权限，有一个全面的IAM教程展示了如何使用标签授予对不同项目和群组的访问权限。

如果您使用SAML基于身份提供商 (IdP) 进行单点登录，则可以将标签附加到为用户提供访问权限的代入角色。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》ABAC中的IAM教程：使用SAML会话标签。

与标签相关的条件密钥

下表描述了可以在IAM权限策略中使用的条件密钥，根据标签控制访问权限。通过这些密钥，您可执行以下操作：

- 比较调用操作的主体上的标签。
- 比较作为参数提供给操作的标签。
- 比较操作将访问的资源所附的标签。

有关条件键及其使用方法的详细信息，请参阅条件密钥名称列中链接的页面。

条件密钥名称	描述
aws:PrincipalTag	将附加到发出请求的委托人（IAM角色或用户）的标签与您在策略中指定的标签进行比较。
aws:RequestTag	将请求中作为参数传递的标签密钥/值对与您在策略中指定的标签密钥/值对进行比较。
aws:ResourceTag	将附加到资源的密钥/值对与您在策略中指定的标签密钥/值对进行比较。
aws:TagKeys	只将请求中的标签密钥与您在策略中指定的密钥进行比较。

使用标签的IAM策略示例

Example 示例 1：强制用户在创建资源时附加特定标签

以下示例IAM权限策略展示了如何强制创建或修改IAM策略标签的用户在密钥Owner中加入标签。此外，该策略要求将标签的值设置为与调用主体所附加的 Owner 标签相同的值。要使此策略发挥作用，所有主体必须附加 Owner 标签，并且必须阻止用户修改该标签。如果尝试创建或修改策略时未包含 Owner 标签，则策略将不匹配，不允许进行操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagCustomerManagedPolicies",
            "Effect": "Allow",
            "Action": [
                "iam:CreatePolicy",
                "iam:TagPolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:policy/*",
            "Condition": {
                "StringEquals": {"aws:RequestTag/Owner": "${aws:PrincipalTag/Owner}"}
            }
        }
    ]
}
```

Example 示例 2：使用标签限制“所有者”对资源的访问权限

以下示例IAM权限策略允许用户停止正在运行的 Amazon EC2 实例，前提是调用委托人使用与该实例相同的`project`标签值进行标记。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances"
      ],
      "Resource": [
        "arn:aws:iam::123456789012:instance/*"
      ],
      "Condition": {
        "StringEquals": {"aws:ResourceTag/project": "${aws:PrincipalTag/project}"}
      }
    }
  ]
}
```

此示例是基于属性的访问控制 () ABAC 的示例。有关使用IAM策略实现基于标签的访问控制策略的更多信息和其他示例，请参阅《AWS Identity and Access Management 用户指南》中的以下主题：

- 使用标签控制对 AWS 资源的访问权限
- 使用标签控制IAM用户和角色的访问权限和访问权限
- IAM教程：根据标签定义访问 AWS 资源的权限-展示如何使用多个标签授予对不同项目和群组的访问权限。

AWS Organizations 标签政策

标签策略是您在中创建的一种策略 AWS Organizations。 您可以使用标签策略来帮助实现组织账户中资源的标签标准化。要使用标签策略，我们建议您按照中标签策略入门中所述的工作流程进行操作 AWS Organizations 用户指南。如该页面所述，建议的工作流程包括查找和更正不合规标签。要完成这些任务，您需要使用标签编辑器控制台。

先决条件和权限

在标签编辑器中评估标签策略的合规性之前，必须满足相应要求并设置必要的权限。

主题

- 评估标签策略合规性的先决条件
- 评估账户合规性的权限
- 评估组织范围合规性的权限
- 使用 Amazon S3 存储桶策略以存储报告

评估标签策略合规性的先决条件

评估标签策略合规性要求以下内容：

- 您必须先在中启用该功能 AWS Organizations，以及创建和附加标签策略。有关更多信息，请参阅中的以下页面 AWS Organizations 用户指南：
  - 管理标签策略的先决条件和权限
  - 启用标签策略
  - 标签策略入门
- 要查找账户资源上的不合规标签，您需要该账户的登录凭证以及 评估账户合规性的权限 中所列权限。
- 要评估组织范围的合规性，您需要组织管理账户的登录凭证以及 评估组织范围合规性的权限 中所列权限。您只能向以下机构索取合规报告 AWS 区域 美国东部（弗吉尼亚北部）。

评估账户合规性的权限

在账户资源上查找不合规标签需要以下权限：

- `organizations:DescribeEffectivePolicy` – 获取账户的有效标签策略的内容。
- `tag:GetResources` – 获取不符合附加标签策略的资源列表。
- `tag:TagResources` – 添加或更新标签。您还需要特定于服务的权限才能创建标签。例如，要在亚马逊弹性计算云 (AmazonEC2) 中为资源添加标签，您需要权限`ec2:CreateTags`。
- `tag:UnTagResources` – 删除标签。您还需要特定于服务的权限才能移除标签。例如，要取消标记 Amazon 中的资源EC2，您需要权限。`ec2:DeleteTags`

以下示例 AWS Identity and Access Management (IAM) 策略提供评估账户标签合规性的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EvaluateAccountCompliance",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeEffectivePolicy",
                "tag:GetResources",
                "tag:TagResources",
                "tag:UnTagResources"
            ],
            "Resource": "*"
        }
    ]
}
```

有关IAM策略和权限的更多信息，请参阅《IAM用户指南》。

评估组织范围合规性的权限

评估组织范围的标签策略合规性需要以下权限：

- `organizations:DescribeEffectivePolicy` – 获取附加到组织、组织单位 (OU) 或账户的标签策略内容。
- `tag:GetComplianceSummary` – 获取组织中所有账户中不合规资源的摘要。
- `tag:StartReportCreation` – 将最近的合规性评估结果导出到文件中。组织级的合规性每隔 48 小时评估一次。
- `tag:DescribeReportCreation` – 检查报告创建的状态。

- `s3:ListAllMyBuckets`— 协助访问组织范围的合规报告。
- `s3:GetBucketAcl`— 检查接收合规报告的 Amazon S3 存储桶的访问控制列表 (ACL)。
- `s3:GetObject`— 从服务拥有的 Amazon S3 存储桶中检索合规报告。
- `s3:PutObject`— 将合规报告放在指定的 Amazon S3 存储桶中。

以下示例IAM策略提供了评估组织范围合规性的权限。替换每个 *placeholder* 用你自己的信息：

- *bucket_name* — 您的亚马逊 S3 存储桶名称
- *organization_id* — 您的组织的 ID

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EvaluateAccountCompliance",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeEffectivePolicy",
                "tag:StartReportCreation",
                "tag:DescribeReportCreation",
                "tag:GetComplianceSummary",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "GetBucketAclForReportDelivery",
            "Effect": "Allow",
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::bucket_name",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "tagpolicies.tag.amazonaws.com"
                }
            }
        },
        {
            "Sid": "GetObjectForReportDelivery",
            "Effect": "Allow",
            "Action": "s3:GetObject",
```

```
            "Resource": "arn:aws:s3:::*/tag-policy-compliance-reports/*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "tagpolicies.tag.amazonaws.com"
                }
            }
        },
        {
            "Sid": "PutObjectForReportDelivery",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::bucket_name/AwsTagPolicies/organization_id/*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "tagpolicies.tag.amazonaws.com"
                },
                "StringLike": {
                    "s3:x-amz-copy-source": "*/tag-policy-compliance-reports/*"
                }
            }
        }
    ]
}
```

有关IAM策略和权限的更多信息，请参阅《IAM用户指南》。

使用 Amazon S3 存储桶策略以存储报告

要创建组织范围的合规报告，您用来调用的身份StartReportCreationAPI必须能够访问美国东部（弗吉尼亚北部）地区的亚马逊简单存储服务 (Amazon S3) Service 存储桶来存储报告。标签策略使用调用身份的凭证将合规性报告传送到指定的存储桶。

如果用于调用的存储桶和身份StartReportCreationAPI属于同一个账户，则此用例不需要其他 Amazon S3 存储桶策略。

如果与用于调用的身份关联的账户与拥有 Amazon S3 存储桶的账户不同，则必须将以下存储桶策略附加到该存储桶。StartReportCreation API替换每个 *placeholder* 用你自己的信息：

- *bucket_name* — 您的亚马逊 S3 存储桶名称
- *organization_id* — 您的组织的 ID
- *##_ ARN* — 用来称呼ARN的IAM身份的 StartReportCreation API

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CrossAccountTagPolicyACL",
            "Effect": "Allow",
            "Principal": {
                "AWS": "identity_ARN"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::bucket_name"
        },
        {
            "Sid": "CrossAccountTagPolicyBucketDelivery",
            "Effect": "Allow",
            "Principal": {
                "AWS": "identity_ARN"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::bucket_name/AwsTagPolicies/organization_id/*"
        }
    ]
}
```

评估账户的合规性

您可以评估组织中的某个账户是否符合其生效标签策略。

> **Important**
>
> 未标记的资源不会在结果中显示为不合规。
> 要在您的账户中查找未标记的资源，请 AWS 资源探索器 与使用的查询一起使用**tag:none**。
> 有关更多信息，请参阅《AWS 资源探索器 用户指南》中的搜索未标记的资源。

生效标签策略指定应用到账户的标记规则。账户继承的任何标签策略以及直接附加到账户的任何标签策略的聚合称为生效标签策略。将标签策略附加到组织根时，它应用到组织中的所有账户。当您将标签策略附加到组织单位 (OU) 时，它适用于属于OUs该组织单位的所有账户。

> **Note**
>
> 如果您尚未创建标签策略，请参阅 AWS Organizations 《用户指南》中的标签策略入门。

要查找不合规标签，您必须拥有以下权限：

- `organizations:DescribeEffectivePolicy`
- `tag:GetResources`
- `tag:TagResources`
- `tag:UntagResources`

评估账户是否符合其生效标签策略（控制台）

1. 登录要检查合规性的账户后，打开标签策略控制台。
2. 生效标签策略部分显示上次策略更新的时间和定义的标签密钥。您可以展开标签密钥，查看有关标签密钥值、案例处理以及是否针对特定资源类型强制使用这些值的信息。

   > **Note**
   >
   > 如果您已登录管理账户，则需要选择一个账户才能查看其生效策略和合规信息。

3. 在带有不合规标签的资源部分中，指定 AWS 区域 要搜索哪些不合规标签。您还可以按资源类型进行搜索。然后选择搜索资源。

   实时结果显示于搜索结果部分。要更改每页返回的结果数或要显示的列，请选择设置图标。
4. 在搜索结果中，选择标签不合规的资源。
5. 在列出资源标签的对话框中，选择超链接以打开已创建资源的 AWS 服务 。在该控制台上，更正不合规标签。

   > **Tip**
   >
   > 如果您不确定哪些标签不合规，请前往标签策略控制台中该账户的生效标签策略部分。您可以展开标签密钥以查看其标记规则。

6. 重复查找和更正标签的过程，直至您所关注的账户资源在每个区域都合规。

要查找不合规的标签 (AWS CLI, AWS API)

使用以下命令和操作查找不合规标签：

- AWS Command Line Interface (AWS CLI):
  - aws resourcegroupstaggingapi get-resources
  - aws resourcegroupstaggingapi tag-resources
  - aws resourcegroupstaggingapi untag-resources

  有关使用标签策略的完整过程 AWS CLI，请参阅《AWS Organizations 用户指南》 AWS CLI中的使用标签策略。
- AWS Resource Groups Tagging API:
  - GetResources
  - TagResources
  - UntagResources

后续步骤

我们建议您重复查找和纠正合规性问题。持续操作，直至您所关注的账户资源符合每个区域的生效标签策略。

查找和更正不合规标签是一个迭代过程，原因众多，其中包括：

- 您的组织对标签策略的使用可能会随着时间推移而发生变化。
- 创建资源时，在组织中进行变更需要时间。
- 每当创建新资源或为资源分配新标签时，合规性就会发生变化。
- 每当账户的标签策略被附加或分离时，该账户的生效标签策略就会更新。每当账户继承的标记策略发生变化时，生效标记策略也会更新。

如果您以组织管理账户的身份登录，还可以生成报告。此报告显示组织账户中所有已标记资源的信息。有关更多信息，请参阅 评估组织级的合规性。

评估组织级的合规性

您可以评估您的组织是否遵守资源的生效标签策略。您能够生成一个报告，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。

> **Important**
>
> 未标记的资源不会在结果中显示为不合规。
> 要在您的账户中查找未标记的资源，请使用 AWS 资源探索器 用一个使用的查询**tag:none**。
> 有关更多信息，请参阅中搜索未标记的资源 AWS 资源探索器 用户指南。

您可以通过您所在组织的管理账户生成报告 us-east-1 AWS 区域 只有。生成报告的账户必须能够访问美国东部（弗吉尼亚州北部）区域中的 Amazon S3 存储桶。存储桶必须具有附加的存储桶策略，如用于存储报告的 Amazon S3 存储桶策略中所示。

要生成组织级的合规性报告，您必须拥有以下权限：

- organizations:DescribeEffectivePolicy
- tag:GetComplianceSummary
- tag:StartReportCreation
- tag:DescribeReportCreation
- s3:ListAllMyBuckets
- s3:GetBucketAcl
- s3:GetObject
- s3:PutObject

有关显示这些权限的IAM策略示例，请查看用于评估组织范围合规性的权限。

生成组织级的合规性报告（控制台）

1. 打开标签策略控制台。
2. 选择此组织根标签，选择生成报告。
3. 在生成报告屏幕上，指定报告的存储位置。
4. 选择开始导出。

报告完成后，您可以从组织根目录选项卡上的不合规报告部分下载报告。

> **注意**
>
> 组织级的合规性每隔 48 小时评估一次。这将产生以下结果：

- 对标签策略或资源所做的更改，最多可能需要 48 小时才能反映在组织级的合规性报告中。例如，假定您有一个标签策略，为某个资源类型定义新的标准化标签。没有此标签的该类型的资源最多需要 48 小时在报告中显示为合规。
- 尽管您可以随时生成报告，但报告结果要等到下一次评估完成后才会更新。
- 该NoncompliantKeys列列出了资源上不符合有效标签策略的标签密钥。
- 该KeysWithNonCompliantValues列列出了资源上有效策略中定义的具有错误案例处理或不合规值的密钥。
- 如果你关闭 AWS 账户 那是该组织的成员，它可以在标签合规报告中持续显示长达 90 天。

要生成组织范围的合规报告 (AWS CLI, AWS API)

使用以下命令和操作生成组织级的合规性报告、检查其状态并查看报告：

- AWS Command Line Interface AWS CLI):
  - aws resourcegroupstaggingapi start-report-creation
  - aws resourcegroupstaggingapi describe-report-creation
  - aws resourcegroupstaggingapi get-compliance-summary

  有关使用标签策略的完整过程，请参阅 AWS CLI，请参阅中的使用标签策略 AWS CLI中的 AWS Organizations 用户指南。
- AWS API:
  - StartReportCreation
  - DescribeReportCreation
  - GetComplianceSummary

使用无服务器工作流程和 Amazon 监控标签更改 EventBridge

Amazon EventBridge 支持对 AWS 资源进行标签更改。使用这种 EventBridge 类型，您可以构建 EventBridge规则以匹配标签更改，并将事件路由到一个或多个目标。例如，目标可能是调用自动化工作流程的 AWS Lambda 函数。本主题提供了一个教程，介绍如何使用 Lambda 构建经济实惠的无服务器解决方案，以安全地处理资源上的标签更改。 AWS

标签更改会生成 EventBridge 事件

EventBridge 提供描述 AWS 资源变化的近乎实时的系统事件流。许多 AWS 资源都支持标签，标签是用户定义的自定义属性，可以轻松组织和分类 AWS 资源。标签的常见使用案例包括成本分配分类、访问控制安全和自动化。

使用 EventBridge，您可以监控标签的更改并跟踪 AWS 资源的标签状态。以前，为了实现类似的功能，您可能需要连续轮询APIs和编排多个呼叫。现在，对标签（包括单个服务APIs、标签编辑器和标记）的任何更改都API将在资源事件中启动标签更改。以下示例显示了标签更改所提示的典型 EventBridge 事件。它显示新的、已更新的或已删除的标签密钥及其关联值。

```
{
  "version": "0",
  "id": "bddcf1d6-0251-35a1-aab0-adc1fb47c11c",
  "detail-type": "Tag Change on Resource",
  "source": "aws.tag",
  "account": "123456789012",
  "time": "2018-09-18T20:41:38Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "a-new-key",
      "an-updated-key",
      "a-deleted-key"
    ],
    "tags": {
      "a-new-key": "tag-value-on-new-key-just-added",
      "an-updated-key": "tag-value-was-just-changed",
      "an-unchanged-key": "tag-value-still-the-same"
    },
```

```
    "service": "ec2",
    "resource-type": "instance",
    "version": 3,
  }
}
```

所有 EventBridge 事件都有相同的顶级字段：

- 版本 – 默认情况下，该值在所有事件中设置为 0 (零)。
- id – 为每个事件生成一个唯一值。在事件通过规则移到目标时以及处理事件时，这对于跟踪事件非常有用。
- 详细信息-类别 – 与 source 字段组合起来标识显示在 detail 字段中的字段和值。
- 来源 – 标识事件来源的服务。标签变更的来源是 aws.tag。
- 时间– 事件发生的时间。
- 区域 – 标识事件源自的 AWS 区域 区域。
- 资源 — 此JSON数组包含 Amazon 资源名称 (ARNs)，用于标识事件中涉及的资源。这是标签已更改的资源。
- detail — 一个JSON对象，其内容因事件类型而异。资源的标签更改包括以下详细字段：
  - changed-tag-keys— 此事件更改的标签密钥。
  - 服务 – 资源所属的服务。在本示例中，服务是ec2，即 Amazon EC2。
  - 资源类别 – 服务的资源类别。在本示例中，它是一个 Amazon EC2 实例。
  - 版本 – 标签集的版本。版本从 1 开始，标签更改时会递增。您可以使用该版本来验证标签更改事件的顺序。
  - 标签 – 更改后附加到资源的标签。

有关更多信息，请参阅亚马逊 EventBridge 用户指南中的亚马逊 EventBridge 事件模式。

通过使用 EventBridge，您可以根据不同的字段创建匹配特定事件模式的规则。我们将在本教程中演示如何执行此操作。此外，我们还将展示在未将指定标签附加到Amazon EC2 实例的情况下如何自动停止该实例。我们使用这些 EventBridge 字段创建模式来匹配启动 Lambda 函数的实例的标签事件。

Lambda 和无服务器

AWS Lambda 遵循无服务器模式在云中运行代码。需要时，您仅需运行代码，无需考虑服务器。您只需按使用的计算时间付费。尽管这种模式被称为无服务器，但这并不意味着没有服务器。在这种情况

下，无服务器意味着您不必预置、配置或管理用于运行代码的服务器。 AWS 所有这些都为你完成，所以你可以专注于你的代码。有关 Lambda 的更多信息，请参阅 AWS Lambda 产品概述。

教程：自动停止缺少所需标签的 Amazon EC2 实例

作为你的水池 AWS 资源和 AWS 账户 你可以管理增长，你可以使用标签来更轻松地对资源进行分类。标签通常用于关键使用案例，例如成本分配和安全性。为了有效管理 AWS 资源，则需要对您的资源进行一致的标记。通常，当资源在配置时会获得所有相应的标签。但是，稍后的流程可能会导致标签变更，从而偏离企业标签策略。通过监控标签变更，您可以发现标签偏差并立即做出响应。这样，对于那些依赖于对资源进行正确分类的流程会产生预期的结果，您就更有信心了。

以下示例演示如何监控 Amazon EC2 实例上的标签更改，以验证指定实例是否继续具有所需的标签。如果实例的标签发生变化并且该实例不再具有所需的标签，则调用 Lambda 函数来自动关闭该实例。您为什么要进行此操作？ 它可以确保根据您的公司标签策略对所有资源进行标记，以实现有效的成本分配，或者能够基于属性的访问控制来信任安全性（ ）ABAC。

> **Important**
>
> 我们强烈建议您在非生产账户中执行本教程，以免无意中关闭重要实例。
> 本教程中的示例代码故意将这种情况的影响限制在实例列表中的实例上IDs。您必须使用愿意关闭以进行测试的实例IDs来更新列表。这有助于确保您不会意外关闭您所在区域中的所有实例 AWS 账户.
> 测试后，请确保根据贵公司的标记策略对所有实例进行标记。然后，您可以删除将函数限制为仅限列表中的实例IDs的代码。

此示例使用 JavaScript 还有 16.x 版本的 Node.js。 该示例使用示例 AWS 账户 ID 123456789012 还有 AWS 区域 美国东部（弗吉尼亚北部）（`us-east-1`）。将这些替换为您自己的测试账户 ID 和区域。

> **Note**
>
> 如果您的控制台默认使用其他区域，请确保在更改控制台时切换了本教程中使用的区域。本教程失败的一个常见原因：实例和函数位于两个不同的区域。

如果您使用的区域与 `us-east-1` 不同，请确保将以下代码示例中的所有引用更改为所选区域。

主题

第 1 步。创建 Lambda 函数

创建 Lambda 函数

1. 打开 AWS Lambda 管理控制台。
2. 选择 创建函数，然后选择 从头开始创作。
3. 对于函数名称，请键入 **AutoEC2Termination**。
4. 对于运行时系统，选择 Node.js 16.x。
5. 将所有其他字段保留为默认值，然后选择创建函数。
6. 在 AutoEC2Termination 详情页面的代码选项卡上，打开 index.js 文件以查看其代码。
   - 如果已打开带有 index.js 的选项卡，则可以在该选项卡中选择编辑框来编辑代码。
   - 如果包含 index.js 的选项卡未打开，请在导航窗格中 “自动” EC2Terminator 文件夹下单击 index.js 文件。然后选择 Open。
7. 在 index.js 选项卡中，将以下代码粘贴到编辑器框中，替换所有已有代码。

   将值 RegionToMonitor 替换为您想要在其中运行此函数的区域。

```
// Set the following line to specify which Region's instances you want to monitor
// Only instances in this Region are succesfully stopped on a match

const RegionToMonitor = "us-east-1"

// Specify the instance ARNs to check.
// This limits the function for safety to avoid the tutorial shutting down all
 instances in account
// The first ARN is a "dummy" that matches the test event you create in Step 3.
// Replace the second ARN with one that matches a real instance that you want to
 monitor and that you can
// safely stop
```

```
const InstanceList = [
    "i-0000000aaaaaaaaaa",
    "i-05db4466d02744f07"
];

// The tag key name and value that marks a "valid" instance. Instances in the
 previous list that
// do NOT have the following tag key and value are stopped by this function

const ValidKeyName = "valid-key";
const ValidKeyValue = "valid-value";

// Load and configure the AWS SDK
const AWS = require('aws-sdk');
// Set the AWS Region
AWS.config.update({region: RegionToMonitor});
// Create EC2 service object.
const ec2 = new AWS.EC2({apiVersion: '2016-11-15'});

exports.handler = (event, context, callback) => {

  // Retrieve the details of the reported event.
  var detail = event.detail;
  var tags = detail["tags"];
  var service = detail["service"];
  var resourceType = detail["resource-type"];
  var resource = event.resources[0];
  var resourceSplit = resource.split("/");
  var instanceId = resourceSplit[resourceSplit.length - 1];

  // If this event is not for an EC2 resource, then do nothing.
  if (!(service === "ec2")) {
    console.log("Event not for correct service -- no action (", service, ")" );
    return;
  }

  // If this event is not about an instance, then do nothing.
  if (!(resourceType === "instance")) {
    console.log("Event not for correct resource type -- no action (", resourceType,
 ")" );
    return;
  }
```

```
 // CAUTION - Removing the following 'if' statement causes the function to run
against
 //           every EC2 instance in the specified Region in the calling AWS ##.
 //           If you do this and an instance is not tagged with the approved tag
key
 //           and value, this function stops that instance.

 // If this event is not for the ARN of an instance in our include list, then do
nothing.
 if (InstanceList.indexOf(instanceId)<0) {
   console.log("Event not for one of the monitored instances -- no action (",
resource, ")");
   return;
 }

 console.log("Tags changed on monitored EC2 instance (",instanceId,")");

 // Check attached tags for expected tag key and value pair
 if ( tags.hasOwnProperty(ValidKeyName) && tags[ValidKeyName] == "valid-value"){
   // Required tags ARE present
   console.log("The instance has the required tag key and value -- no action");
   callback(null, "no action");
   return;
 }

 // Required tags NOT present
 console.log("This instance is missing the required tag key or value -- attempting
to stop the instance");

 var params = {
   InstanceIds: [instanceId],
   DryRun: true
 };

 // call EC2 to stop the selected instances
 ec2.stopInstances(params, function(err, data) {
   if (err && err.code === 'DryRunOperation') {
     // dryrun succeeded, so proceed with "real" stop operation
     params.DryRun = false;
     ec2.stopInstances(params, function(err, data) {
       if (err) {
         console.log("Failed to stop instance");
         callback(err, "fail");
       } else if (data) {
```

```
            console.log("Successfully stopped instance", data.StoppingInstances);
            callback(null, "Success");
          }
        });
      } else {
        console.log("Dryrun attempt failed");
        callback(err);
      }
    });
};
```

8. 选择部署以保存您的更改并激活新版本函数。

此 Lambda 函数会检查中标签更改事件所报告的亚马逊EC2实例的标签。 EventBridge在此示例中，如果事件中的实例缺少所需的标签密钥 `valid-key` 或该标签没有值 `valid-value`，则该函数会尝试停止该实例。您可以根据自己的特定用例更改此逻辑检查或标签要求。

使 Lambda 控制台浏览器窗口保持打开状态。

第 2 步。设置所需的IAM权限

在函数成功运行之前，您必须向该函数授予停止EC2实例的权限。这些区域有： AWS 提供的角色 lambda_basic_execution没有该权限。在本教程中，您将修改附加到名为的函数执行角色的默认IAM权限策略`AutoEC2Termination-role-`*`uniqueid`*。本教程所需的最低额外权限为 `ec2:StopInstances`。

有关创建亚马逊EC2特定IAM策略的更多信息，请参阅《IAM用户指南》中的 “AmazonEC2：允许以编程方式启动或停止EC2实例以及修改安全组”。

创建IAM权限策略并将其附加到 Lambda 函数的执行角色

1. 在不同的浏览器选项卡或窗口中，打开IAM控制台的 “角色” 页面。
2. 开始键入角色名称 **`AutoEC2Termination`** ，当角色名称出现在列表中时，选择角色名称。
3. 在角色的摘要页面上，选择权限选项卡，然后选择已附加的一个策略的名称。
4. 在策略的摘要页面上，选择 编辑策略。
5. 在可视化编辑器选项卡上，选择添加额外权限。
6. 对于 Service，选择 EC2。
7. 在 “操作” 中，选择StopInstances。您可以在搜索栏中键入 **`Stop`** ，在它出现时选中 `StopInstances`。

8. 对于资源，选择所有资源，选择检查策略，然后选择保存更改。

   这将自动创建新版本的策略并将该版本设置为默认版本。

   您的最终策略应类似于以下示例。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:StopInstances",
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": "logs:CreateLogGroup",
            "Resource": "arn:aws:logs:us-east-1:123456789012:*"
        },
        {
            "Sid": "VisualEditor2",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:us-east-1:123456789012:log-group:/aws/lambda/
AutoEC2Termination:*"
        }
    ]
}
```

第 3 步。对您的 Lambda 函数进行初步测试

在本步骤中，您将向函数提交测试事件。Lambda 测试功能通过提交手动提交的测试事件来运行。该函数处理测试事件，就像事件来自一样 EventBridge。您可以定义多个具有不同值的测试事件，以测试代码的各个不同部分。在此步骤中，您将提交一个测试事件，该事件表明 Amazon EC2 实例的标签已更改，并且新标签不包含所需的标签键和值。

测试 Lambda 函数

1. 使用 Lambda 控制台返回窗口或选项卡，然后打开自动EC2Termination函数的 “测试” 选项卡。
2. 选择 创建新事件。
3. 对于事件名称，输入 **SampleBadTagChangeEvent**。
4. 在事件中JSON，将文本替换为以下示例文本中显示的示例事件。您无需修改账户、地区或实例 ID，此测试事件即可正常运行。

```
{
  "version": "0",
  "id": "bddcf1d6-0251-35a1-aab0-adc1fb47c11c",
  "detail-type": "Tag Change on Resource",
  "source": "aws.tag",
  "account": "123456789012",
  "time": "2018-09-18T20:41:38Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "valid-key"
    ],
    "tags": {
      "valid-key": "NOT-valid-value"
    },
    "service": "ec2",
    "resource-type": "instance",
    "version": 3
  }
}
```

5. 选择 Save（保存），然后选择 Test（测试）。

   测试似乎失败了，但没关系。

   您应该会在响应下的执行结果选项卡中看到以下错误。

```
{
  "errorType": "InvalidInstanceID.NotFound",
  "errorMessage": "The instance ID 'i-0000000aaaaaaaaaa' does not exist",
  ...
```

```
}
```

之所以出现错误，是因为测试事件中指定的实例不存在。

函数日志部分的 “执行结果” 选项卡上的信息表明，您的 Lambda 函数成功尝试停止实例EC2。但是，它失败了，因为代码最初尝试执行停止实例的 DryRun 操作，这表明实例 ID 无效。

```
START RequestId: 390c1f8d-0d9b-4b44-b087-8de64479ab44 Version: $LATEST
2022-11-30T20:17:30.427Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    INFO    Tags
 changed on monitored EC2 instance ( i-0000000aaaaaaaaaa )
2022-11-30T20:17:30.427Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    INFO    This
 instance is missing the required tag key or value -- attempting to stop the
 instance
2022-11-30T20:17:31.206Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    INFO    Dryrun
 attempt failed
2022-11-30T20:17:31.207Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    ERROR   Invoke
 Error     {"errorType":"InvalidInstanceID.NotFound","errorMessage":"The instance
 ID 'i-0000000aaaaaaaaaa' does not
 exist","code":"InvalidInstanceID.NotFound","message":"The instance ID
 'i-0000000aaaaaaaaaa' does not
 exist","time":"2022-11-30T20:17:31.205Z","requestId":"a5192c3b-142d-4cec-
bdbc-685a9b7c7abf","statusCode":400,"retryable":false,"retryDelay":36.87870631147607,"stack
["InvalidInstanceID.NotFound: The instance ID 'i-0000000aaaaaaaaaa' does
 not exist","    at Request.extractError (/var/runtime/node_modules/aws-sdk/
lib/services/ec2.js:50:35)","    at Request.callListeners (/var/runtime/
node_modules/aws-sdk/lib/sequential_executor.js:106:20)","    at Request.emit
 (/var/runtime/node_modules/aws-sdk/lib/sequential_executor.js:78:10)","    at
 Request.emit (/var/runtime/node_modules/aws-sdk/lib/request.js:686:14)","    at
 Request.transition (/var/runtime/node_modules/aws-sdk/lib/request.js:22:10)","
    at AcceptorStateMachine.runTo (/var/runtime/node_modules/aws-sdk/lib/
state_machine.js:14:12)","    at /var/runtime/node_modules/aws-sdk/lib/
state_machine.js:26:10","    at Request.<anonymous> (/var/runtime/node_modules/aws-
sdk/lib/request.js:38:9)","    at Request.<anonymous> (/var/runtime/node_modules/
aws-sdk/lib/request.js:688:12)","    at Request.callListeners (/var/runtime/
node_modules/aws-sdk/lib/sequential_executor.js:116:18)"]}
END RequestId: 390c1f8d-0d9b-4b44-b087-8de64479ab44
```

6. 要证明代码在使用正确标签时不会尝试停止实例，您可以创建并提交另一个测试事件。

   选择代码源上方的测试选项卡。控制台显示您现有的SampleBadTagChangeEvent测试事件。

7. 选择 创建新事件。

8. 对于事件名称，键入 **SampleGoodTagChangeEvent**。

9. 在第 17 行中，删除 **NOT-**，将值更改为 **valid-value**。
10. 在测试事件窗口的顶部，选择保存，然后选择测试。

    输出显示以下内容，这表明该函数可以识别有效标签并且不会尝试关闭实例。

```
START RequestId: 53631a49-2b54-42fe-bf61-85b9e91e86c4 Version: $LATEST
2022-12-01T23:24:12.244Z    53631a49-2b54-42fe-bf61-85b9e91e86c4    INFO    Tags
 changed on monitored EC2 instance ( i-0000000aaaaaaaaaa )
2022-12-01T23:24:12.244Z    53631a49-2b54-42fe-bf61-85b9e91e86c4    INFO    The
 instance has the required tag key and value -- no action
END RequestId: 53631a49-2b54-42fe-bf61-85b9e91e86c4
```

    在浏览器中保持 Lambda 控制台处于打开状态。

第 4 步。创建启动函数的 EventBridge 规则

现在，您可以创建与事件匹配并指向您的 Lambda 函数的 EventBridge 规则。

创建 EventBridge 规则

1. 在其他浏览器选项卡或窗口中，打开EventBridge 控制台，进入 “创建规则” 页面。
2. 在名称中，输入 **ec2-instance-rule**，然后选择下一步。
3. 向下滚动到 “创建方法”，然后选择 “自定义模式（JSON编辑器）”。
4. 在编辑框中，粘贴以下图案文本，然后选择下一步。

```
{
  "source": [
    "aws.tag"
  ],
  "detail-type": [
    "Tag Change on Resource"
  ],
  "detail": {
    "service": [
      "ec2"
    ],
    "resource-type": [
      "instance"
    ]
  }
```

```
}
```

此规则Tag Change on Resource会匹配 Amazon EC2 实例的事件，并在下一步中调用您指定为 Targ et 的任何内容。

5. 接下来，将 Lambda 函数添加为目标。在目标 1框中，在选择目标下，选择 Lambda 函数。
6. 在 “函数” 下，选择您之前创建的 “自动” EC2Termination 函数，然后选择 “下一步”。
7. 请在 配置标签页面上，选择 下一步。然后，请在 审核和创建页面上，选择 创建规则。这还会自动授予调用 EventBridge 指定 Lambda 函数的权限。

第 5 步。测试完整的解决方案

您可以通过创建EC2实例并观察更改其标签时会发生什么来测试最终结果。

使用真实实例测试监控解决方案

1. 打开 A mazon EC2 控制台，进入实例页面。
2. 创建一个 Amazon EC2 实例。在启动之前，请附加带有密钥 valid-key 和值 valid-value 的标签。有关如何创建和启动实例的信息，请参阅 Amazon EC2 用户指南中的步骤 1：启动实例。在启动实例的过程中，在步骤 3 中，输入名称标签，还要选择添加额外标签，选择添加标签，然后输入密钥 **valid-key** 和值 **valid-value**。如果此实例仅用于本教程，并且您计划在完成后删除此实例，您可以在没有密钥对的情况下继续。完成步骤 1 后，返回本教程即可，您无需执行步骤 2：连接到实例。
3. InstanceId从控制台复制。
4. 从亚马逊EC2控制台切换到 Lambda 控制台。选择您的自动EC2Termination功能，选择代码选项卡，然后选择 index.js 选项卡来编辑您的代码。
5. InstanceList通过粘贴您从 Amazon EC2 控制台复制的值来更改中的第二个条目。确保该 RegionToMonitor 值与包含您粘贴的实例的区域相匹配。
6. 选择部署以激活您的更改。现在，该函数已准备就绪，可以通过在指定区域对该实例进行标签更改来激活。
7. 从 Lambda 控制台切换到亚马逊EC2控制台。
8. 通过删除有效密钥标签或更改该密钥的值来更改附加到实例的标签。

> **Note**
>
> 有关如何在正在运行的亚马逊EC2实例上更改标签的信息，请参阅亚马逊EC2用户指南中的在单个资源上添加和删除标签。

9. 等待几秒钟，然后刷新控制台。该实例应将其实例状态更改为正在停止，然后更改为已停止。
10. 使用您的函数从 Amazon EC2 控制台切换到 Lambda 控制台，然后选择监控选项卡。
11. 选择 “日志” 选项卡，然后在 “最近的调用” 表中选择该列中的最新条目。LogStream

    Amazon CloudWatch 控制台会打开您的 Lambda 函数的最后一次调用的日志事件页面。最后一条条目应类似于以下示例。

```
2022-11-30T12:03:57.544-08:00    START RequestId: b5befd18-2c41-43c8-
a320-3a4b2317cdac Version: $LATEST
2022-11-30T12:03:57.548-08:00    2022-11-30T20:03:57.548Z b5befd18-2c41-43c8-
a320-3a4b2317cdac INFO Tags changed on monitored EC2 instance ( arn:aws:ec2:us-
west-2:123456789012:instance/i-1234567890abcdef0 )
2022-11-30T12:03:57.548-08:00    2022-11-30T20:03:57.548Z b5befd18-2c41-43c8-
a320-3a4b2317cdac INFO This instance is missing the required tag key or value --
 attempting to stop the instance
2022-11-30T12:03:58.488-08:00    2022-11-30T20:03:58.488Z b5befd18-2c41-43c8-
a320-3a4b2317cdac INFO Successfully stopped instance [ { CurrentState: { Code: 64,
 Name: 'stopping' }, InstanceId: 'i-1234567890abcdef0', PreviousState: { Code: 16,
 Name: 'running' } } ]
2022-11-30T12:03:58.546-08:00    END RequestId: b5befd18-2c41-43c8-
a320-3a4b2317cdac
```

教程摘要

本教程演示了如何为Amazon EC2 实例创建与资源事件的标签更改相匹配的 EventBridge 规则。该规则指向一个 Lambda 函数，如果实例没有所需的标签，该函数会自动关闭该实例。

Amazon EventBridge 支持更改标签 AWS 资源为在许多领域构建事件驱动的自动化开辟了可能性 AWS 服务。 将此功能与 AWS Lambda 为您提供构建可访问的无服务器解决方案的工具 AWS 资源安全、按需扩展，且具有成本效益。

该 tag-change-on-resource EventBridge 活动的其他可能用例包括：

- 如果有人从异常 IP 地址访问您的资源，会发出警告 – 使用标签，储存访问您的资源的每位访客的源 IP 地址。对标签的更改会生成一个 CloudWatch 事件。您可以使用该事件将源 IP 地址与有效 IP 地址列表进行比较，并在源 IP 地址无效时激活警告电子邮件。
- 监控资源的基于标签的访问控制是否发生了变化 — 如果您使用基于属性（标签）的访问控制 (ABAC) 设置了对资源的访问权限，则可以使用对标签进行任何更改所生成 EventBridge的事件来提示您的安全团队进行审计。

对标签更改进行故障排除

如果尝试在查找要添加标签的资源查询结果中的选定资源上应用或更改标签时出现错误，以下核对清单可能是非常有用的。

- 资源可能已具有最大数量的标签。通常，资源最多可以有 50 个用户定义的标签。 AWS 生成的标签不计入 50 个标签的最大值。其他用户可能也同时将标签添加到同一资源，这可能会将资源的标签数增加到最大值。
- 某些服务允许在创建标签时使用不同的字符集（或限制允许的字符集）。如果使用特殊字符添加或更改了标签，请查看资源的服务文档中的标签要求以确认服务允许使用这些字符。
- 您可能无修改资源标签的权限。如果您没有权限查看资源上的现有标签，则无法对资源的标签进行更改。
- 您可能没有权限以更改资源。更改资源的元数据可能会受到另一个管理员的限制。
- 另一个用户或进程可能已编辑或删除资源。例如，假设在创建 AWS CloudFormation 堆栈的过程中启动了一个资源。如果堆栈已删除或不再处于活动状态，则该资源可能不再可用。
- 如果资源脱机或终止，或者正在对资源进行其他更新（如软件升级），则可能无法更改标签。
- 如果在标签更改完成之前关闭浏览器选项卡或更改页面，标签更改可能会失败。在离开页面之前，完成标签更改，并等待在页面上显示成功或失败横幅。
- 虽然有速率限制，但你要标记的服务可能会施加一个单独的限制 AWS Resource Groups Tagging API，你可能会在 Resource Groups Tagging API 限制之前达到这个限制。

重试失败的标签更改

如果标签更改在至少一个选定的资源上失败，标签编辑器将在页面底部显示一个红色横幅。横幅显示发生的每种类型的失败的错误消息。对于每个错误，横幅指定标签编辑器无法更改标签的特定资源。在查看并解决错误后，请选择在资源上重试失败的标签更改以仅在标签更改失败的那些资源上重试更改。

标签编辑器的安全性

AWS 十分重视云安全性。作为 AWS 客户，您将从专为满足大多数安全敏感型企业的要求而打造的数据中心和网络架构中受益。

安全性是 AWS 和您的共同责任。责任共担模式将其描述为云的 安全性和云中 的安全性：

- 云的安全性 – AWS 负责保护在 AWS Cloud 中运行 AWS 服务的基础设施。AWS 还向您提供可安全使用的服务。作为 AWS 合规性计划的一部分，第三方审核人员将定期测试和验证安全性的有效性。关于适用于标签编辑器的合规性计划的更多信息，请参阅 合规性计划范围内的 AWS 服务。
- 云中的安全性 - 您的责任由您使用的 AWS 服务 决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

此文档将帮助您了解如何在使用标签编辑器时应用责任共担模式。以下主题说明如何配置标签编辑器以实现您的安全性和合规性目标。

主题

标签编辑器的数据保护

这些区域有： AWS 分担责任模型适用于标签编辑器中的数据保护。如本模型所述， AWS 负责保护运行所有内容的全球基础设施 AWS Cloud。 您有责任保持对托管在此基础架构上的内容的控制。您还负责以下各项的安全配置和管理任务 AWS 服务 你用的。有关数据隐私的更多信息，请参阅数据隐私 FAQ。 有关欧洲数据保护的信息，请参阅 AWS 责任共担模型和GDPR博客文章 AWS 安全博客。

出于数据保护的目的，我们建议您进行保护 AWS 账户 凭据并使用设置个人用户 AWS IAM Identity Center 或者 AWS Identity and Access Management (IAM)。这样，每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证 (MFA)。

- 使用SSL/TLS与之通信 AWS 资源的费用。我们需要 TLS 1.2，建议使用 TLS 1.3。
- 使用API进行设置和用户活动记录 AWS CloudTrail。 有关使用 CloudTrail 轨迹进行捕获的信息 AWS 活动，请参阅使用中的 CloudTrail 轨迹 AWS CloudTrail 用户指南。
- 使用 AWS 加密解决方案，以及其中的所有默认安全控件 AWS 服务.
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在访问时需要 FIPS 140-3 经过验证的加密模块 AWS 通过命令行界面或API，使用FIPS端点。有关可用FIPS端点的更多信息，请参阅联邦信息处理标准 (FIPS) 140-3。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括当你使用标签编辑器或其他工具时 AWS 服务 使用控制台API， AWS CLI，或 AWS SDKs。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您URL向外部服务器提供，我们强烈建议您不要在中包含凭据信息，URL以验证您对该服务器的请求。

数据加密

标记信息未加密。尽管标签未加密，但其可能包含作为安全策略一部分的信息，因此控制谁可以访问资源上的标签非常重要。控制谁可以修改标签尤其重要，因为这类访问可用于提升个人权限。

静态加密

没有其他方法可以隔离标签编辑器特有的服务或网络流量。如果适用，请使用 AWS 特定的隔离。您可以在虚拟私有云 (VPC) 中使用标签编辑APIAPI器和控制台，以帮助最大限度地提高隐私和基础架构的安全性。

传输中加密

标签编辑器数据在传输到服务的内部数据库进行备份时会进行加密。用户无法对其进行配置。

密钥管理

标签编辑器目前未与集成 AWS Key Management Service 并且不支持 AWS KMS keys.

互联网络流量隐私保护

标签编辑器HTTPS用于标签编辑器用户和用户之间的所有传输 AWS。 标签编辑器使用传输层安全 (TLS) 1.3，但也支持 TLS 1.2。

适用于标签编辑器的身份和访问管理

AWS Identity and Access Management (IAM) AWS 服务 可以帮助管理员安全地控制对 AWS 资源的访问权限。IAM管理员控制谁可以进行身份验证（登录）和授权（有权限）使用标签编辑器资源。IAM无需支付额外费用即可使用。 AWS 服务

主题

受众

使用 AWS Identity and Access Management (IAM) 的方式会有所不同，具体取决于您在标签编辑器中所做的工作。

服务用户 – 如果使用标签编辑器服务来完成任务，则您的管理员会为您提供所需的凭证和权限。当您使用更多标签编辑器特征来完成工作时，您可能需要额外权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问标签编辑器中的特征，请参阅对标签编辑器身份和访问进行故障排除。

服务管理员 – 如果您在公司负责标签编辑器资源，则您可能具有标签编辑器的完全访问权限。您有责任确定您的服务用户应访问哪些标签编辑器特征和资源。然后，您必须向IAM管理员提交更改服务用户权限的请求。查看此页面上的信息以了解的基本概念IAM。要详细了解贵公司如何IAM使用标签编辑器，请参阅标签编辑器的工作原理 IAM。

IAM管理员-如果您是IAM管理员，则可能需要详细了解如何编写策略来管理对标签编辑器的访问权限。要查看可在中使用的标签编辑器基于身份的策略示例IAM，请参阅。标签编辑器基于身份的策略示例

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 AWS 账户根用户、IAM用户身份或通过担任IAM角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （ IAM身份中心）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员之前使用IAM角色设置了联合身份。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅IAM用户指南中的签署 AWS API请求。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如， AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅用户指南中的多重身份验证和AWS IAM Identity Center 用户指南 AWS中的使用多因素身份验证 (MFA)。IAM

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关需要您以 root 用户身份登录的任务的完整列表，请参阅《用户指南》中的 “需要根用户凭据的IAM任务”。

用户和组

IAM用户是您内部 AWS 账户 对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时证书，而不是创建拥有密码和访问密钥等长期凭证的IAM用户。但是，如果您有需要IAM用户长期凭证的特定用例，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM用户指南》中的定期轮换需要长期凭证的用例的访问密钥。

IAM群组是指定IAM用户集合的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可以拥有一个名为的群组，IAMAdmins并授予该群组管理IAM资源的权限。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM用户指南》中的何时创建IAM用户（而不是角色）。

角色

IAM角色是您内部具有特定权限 AWS 账户 的身份。它与IAM用户类似，但与特定人员无关。您可以 AWS Management Console 通过切换IAM角色在中临时扮演角色。您可以通过调用 AWS CLI 或 AWS API操作或使用自定义操作来代入角色URL。有关使用角色的方法的更多信息，请参阅《IAM用户指南》中的代入角色的方法。

IAM具有临时证书的角色在以下情况下很有用：

- 联合用户访问 – 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关用于联合身份验证的角色的信息，请参阅《IAM用户指南》中的为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为了控制您的身份在进行身份验证后可以访问的内容，Ident IAM ity Center 会将权限集关联到中的IAM角色。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的 权限集。
- 临时IAM用户权限-IAM 用户或角色可以代入一个IAM角色，为特定任务临时获得不同的权限。
- 跨账户访问-您可以使用IAM角色允许其他账户中的某人（受信任的委托人）访问您账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解角色和基于资源的跨账户访问策略之间的区别，请参阅IAM用户指南IAM中的跨账户资源访问权限。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在服务中拨打电话时，该服务通常会在 Amazon 中运行应用程序EC2或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS)-当您使用IAM用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS使用调用委托人的权限 AWS 服务以及 AWS 服务 向下游服务发出请求的请求。FAS只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出请求。在这种情况下，您必须具有执行这两个操作的权限。有关提出FAS请求时的政策详情，请参阅转发访问会话。
  - 服务角色-服务IAM角色是服务代替您执行操作的角色。IAM管理员可以在内部创建、修改和删除服务角色IAM。有关更多信息，请参阅《IAM用户指南》 AWS 服务中的创建角色以向委派权限。
  - 服务相关角色-服务相关角色是一种与服务相关联的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM管理员可以查看但不能编辑服务相关角色的权限。
- 在 Amazon 上运行的应用程序 EC2 — 您可以使用IAM角色管理在EC2实例上运行并发出 AWS CLI 或 AWS API请求的应用程序的临时证书。这比在EC2实例中存储访问密钥更可取。要为EC2实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建一个附加到该实例的实例配置文件。实例

配置文件包含该角色，并允许在EC2实例上运行的程序获得临时证书。有关更多信息，请参阅IAM用户指南中的使用IAM角色向在 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用IAM角色还是使用IAM用户，请参阅《用户指南》中的何时创建IAM角色（而不是IAM用户）。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以JSON文档的 AWS 形式存储在中。有关JSON策略文档结构和内容的更多信息，请参阅《IAM用户指南》中的JSON策略概述。

管理员可以使用 AWS JSON策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对其所需资源执行操作的权限，IAM管理员可以创建IAM策略。然后，管理员可以将IAM策略添加到角色中，用户可以代入这些角色。

IAM无论您使用何种方法执行操作，策略都会定义该操作的权限。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或获取角色信息 AWS API。

基于身份的策略

基于身份的策略是可以附加到身份（例如IAM用户、用户组或角色）的JSON权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅IAM用户指南中的创建IAM策略。

基于身份的策略可以进一步归类为内联策略或托管策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管策略或内联策略之间进行选择，请参阅《IAM用户指南》中的在托管策略和内联策略之间进行选择。

基于资源的策略

基于资源的JSON策略是您附加到资源的策略文档。基于资源的策略的示例包括IAM角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资

源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略IAM中使用 AWS 托管策略。

访问控制列表 (ACLs)

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。ACLs与基于资源的策略类似，尽管它们不使用JSON策略文档格式。

Amazon S3 AWS WAF、和亚马逊VPC就是支持的服务示例ACLs。要了解更多信息ACLs，请参阅《亚马逊简单存储服务开发者指南》中的访问控制列表 (ACL) 概述。

其他策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界-权限边界是一项高级功能，您可以在其中设置基于身份的策略可以向IAM实体（IAM用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅《IAM用户指南》中的IAM实体的权限边界。
- 服务控制策略 (SCPs)-SCPs 是为中的组织或组织单位 (OU) 指定最大权限的JSON策略 AWS Organizations。 AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有账户。对成员账户中的实体（包括每个实体）的权限进行了SCP限制 AWS 账户根用户。有关 Organization SCPs s 和的更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略。
- 会话策略 – 会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅《IAM用户指南》中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅IAM用户指南中的策略评估逻辑。

标签编辑器的工作原理 IAM

在使用IAM管理标签编辑器的访问权限之前，您应该了解标签编辑器可以使用哪些IAM功能。要全面了解标签编辑器和其他工具是如何使用 AWS 服务 的 IAM AWS 服务 ，请参阅《IAM用户指南》IAM中的使用方法。

主题

标签编辑器基于身份的策略

使用IAM基于身份的策略，除了允许或拒绝操作的条件外，您还可以指定允许或拒绝的操作和资源。标签编辑器支持特定的操作、资源和条件键。要了解您在JSON策略中使用的所有元素，请参阅IAM用户指南中的IAMJSON策略元素参考。

操作

管理员可以使用 AWS JSON策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源执行操作，以及在什么条件下执行。

JSON策略Action元素描述了可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API操作同名。也有一些例外，例如没有匹配API操作的仅限权限的操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

标签编辑器中的策略操作在操作前使用以下前缀：tag:。标签编辑器操作完全在控制台中执行，但在日志条目中带有前缀 tag。

例如，要授予某人使用该操作标记资源的权限，您需要将该tag:TagResourcesAPItag:TagResources操作包含在他们的策略中。策略语句必须包含 Action 或 NotAction 元素。标签编辑器定义了一组自己的操作，以描述您可以使用该服务执行的任务。

要在单个语句中指定多项标签操作，请使用逗号将它们隔开，如下所示。

```
"Action": [
```

```
        "tag:action1",
        "tag:action2",
        "tag:action3"
```

您也可以使用通配符 (*) 指定多个操作。例如，要指定以单词 Get 开头的所有操作，请包括以下操作。

```
"Action": "tag:Get*"
```

要查看标签编辑器操作的列表，请参阅《服务授权参考》中的 标签编辑器的操作、资源和条件密钥。

资源

管理员可以使用 AWS JSON策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源执行操作，以及在什么条件下执行。

ResourceJSON策略元素指定要应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。最佳做法是，使用资源的 Amazon 资源名称 (ARN) 来指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"
```

标签编辑器本身没有任何资源。它操纵的是附加到其他 AWS 服务创建的资源上的元数据（标签）。

条件键

管理员可以使用 AWS JSON策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在资源上标有IAM用户的用户名时，您才能向IAM用户授予访问该资源的权限。有关更多信息，请参阅《IAM用户指南》中的IAM策略元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件键。要查看所有 AWS 全局条件键，请参阅IAM用户指南中的AWS 全局条件上下文密钥。

标签编辑器不规定任何特定于服务的条件密钥。

示例

要查看标签编辑器基于身份的策略的示例，请参阅标签编辑器基于身份的策略示例。

基于资源的策略

标签编辑器不支持基于资源的策略，因为其未定义自身的任何资源。

基于标签的授权

基于标签的授权是称为基于属性的访问控制 () ABAC 的安全策略的一部分。

要基于标签控制对资源的访问，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件密钥在策略的条件元素中提供标签信息。在创建或更新资源时，可以对资源应用标签。

要查看基于身份的策略（用于根据资源上的标签来限制对该资源的访问）的示例，请参阅根据标签查看组。有关基于属性的访问控制 (ABAC) 的更多信息，请参阅用途是什么ABAC？ AWS 在《IAM用户指南》中。

标签编辑器IAM角色

IAM角色是您内部具有特定权限 AWS 账户 的实体。标签编辑器没有或不使用服务角色。

将临时凭证用于标签编辑器

在标签编辑器中，您可以使用临时证书通过联合身份登录、代入IAM角色或担任跨账户角色。您可以通过调用AssumeRole或之类的 AWS STS API操作来获取临时安全证书GetFederationToken。

服务相关角色

服务相关角色 AWS 服务 允许访问其他服务中的资源以代表您完成操作。

标签编辑器没有且不使用服务相关角色。

服务角色

此功能允许服务代表您担任服务角色。

标签编辑器没有或不使用服务角色。

标签编辑器基于身份的策略示例

默认情况下，诸如角色和用户之类的 IAM 主体没有创建或修改标签的权限。它们还无法使用 AWS Management Console、AWS Command Line Interface（AWS CLI）或 AWSAPI 执行任务。IAM 管理员必须创建 IAM policy，以便为主体授予权限以对所需的指定资源执行特定的 API 操作。然后，管理员必须将这些策略附加到需要这些权限的主体。

要了解如何使用这些示例 JSON 策略文档创建 IAM 基于身份的策略的说明，请参阅《IAM 用户指南》中的 在 JSON 选项卡上创建策略。

主题

策略最佳实践

基于身份的策略确定某个人是否可以创建、访问或删除您账户中的标签编辑器资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- AWS 托管策略及转向最低权限许可入门 – 要开始向用户和工作负载授予权限，请使用 AWS 托管策略来为许多常见使用场景授予权限。您可以在 AWS 账户中找到这些策略。建议通过定义特定于您的使用场景的 AWS 客户管理型策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管策略 或 工作职能的 AWS 托管策略。
- 应用最低权限 – 在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限 – 您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果通过特定 AWS 服务（例如 AWS CloudFormation）使用服务操作，您还可以使用条件来授予对服务操作的访问权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言 (JSON) 和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，有助于制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM Access Analyzer 策略验证。

- 需要多重身份验证 (MFA) – 如果您所处的场景要求您的 AWS 账户 中有 IAM 用户或根用户，请启用 MFA 来提高安全性。要在调用 API 操作时要求 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的配置受 MFA 保护的 API 访问。

有关 IAM 中的最佳实践的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。

使用标签编辑器控制台和资源组标记 API

要访问标签编辑器控制台和资源组标记 API，您必须具有一组最低的权限。这些权限必须允许您在您的 AWS 账户 列出和查看关于附加到资源上的标签编辑器的详细信息。如果创建比必需的最低权限更为严格的基于身份的策略，对于带有该策略的 IAM 主体，控制台和 API 命令将无法按预期正常运行。

为确保这些主体仍然可以使用标签编辑器，请将以下策略（或包含以下策略所列权限的策略）附加到实体中。有关更多信息，请参阅 IAM 用户指南中的为用户添加权限：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-explorer:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

有关授予标签编辑器和资源组标记 API 的访问权限的更多信息，请参阅 授予使用标签编辑器的权限。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联策略和托管式策略。此策略包括在控制台上完成此操作或者以编程方式使用 AWS CLI 或 AWS API 所需的权限。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

根据标签查看组

您可以在基于身份的策略中使用条件，以便基于标签控制对标签编辑器资源的访问。该示例说明了如何创建策略以允许查看资源（在该示例中，是资源组）。但是，仅当组标签 `project` 与附加在发出调用的主体上的 `project` 标签具有相同值时，才会授予权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": "resource-groups:ListGroups",
            "Resource": "arn:aws:resource-groups::region:account_ID:group/group_name"
        },
        {
            "Effect": "Allow",
            "Action": "resource-groups:ListGroups",
            "Resource": "arn:aws:resource-groups::region:account_ID:group/group_name",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/project": "${aws:PrincipalTag/
project}"}
            }
        }
    ]
}
```

您可以将此策略附加到您账户中的用户。如果具有标签密钥 `project` 和标签值 `alpha` 的用户尝试查看资源组，还必须对该组标记 `project=alpha`。否则，该用户将被拒绝访问。条件标签键 `project` 匹配 `Project` 和 `project`，因为条件键名称不区分大小写。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。

对标签编辑器身份和访问进行故障排除

使用以下信息可帮助您诊断和修复在使用标签编辑器和 IAM 时可能遇到的常见问题。

主题

- 我无权在标签编辑器中执行操作
- 我无权执行 iam：PassRole

我无权在标签编辑器中执行操作

如果 AWS Management Console 告诉您，您无权执行某个操作，则必须联系您的管理员寻求帮助。管理员是向您提供登录凭证的人。

当 `mateojackson` 用户尝试使用控制台查看资源上的标签，但不具有`tag:GetTagKeys`权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 tag:GetTagKeys on resource: arn:aws:resource-groups::us-west-2:123456789012:resource-
type/my-test-resource
```

在这种情况下，Mateo 请求他的管理员更新其策略，以允许他使用 `tag:GetTagKeys` 操作访问 `my-test-resource` 资源。

我无权执行 iam：PassRole

如果您收到一个错误，表明您无权执行 `iam:PassRole` 操作，则必须更新策略以允许您将角色传递给标签编辑器。

有些 AWS 服务 允许将现有角色传递到该服务，而不是创建新服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 `marymajor` 的 IAM 用户尝试使用控制台在标签编辑器中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。

如果您需要帮助，请联系 AWS 管理员。您的管理员是提供登录凭证的人。

标签编辑器的日志记录和监控

所有标签编辑器操作均已记录在 AWS CloudTrail 中。

使用记录标签编辑器 API 调用 CloudTrail

标签编辑器与AWS CloudTrail一项服务集成，该服务提供用户、角色或标签编辑器AWS 服务中执行的操作的记录。 CloudTrail 将标签编辑器的所有 API 调用捕获为事件，包括来自标签编辑器控制台的调用和对 Resource Groups Tagging API 的代码调用。如果您创建跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括标签编辑器的事件。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的 “事件历史记录” 中查看最新的事件。使用收集的信息 CloudTrail，您可以确定向标签编辑器发出的请求、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

有关的更多信息 CloudTrail，请参阅《AWS CloudTrail用户指南》。

中的标签编辑器信息 CloudTrail

CloudTrail 在您创建账户AWS 账户时已在您的账户上启用。当活动发生在标签编辑器或标签编辑器控制台中时，该活动会与其他 CloudTrail事件一起记录在AWS 服务事件历史记录中。您可以在 AWS 账户 中查看、搜索和下载最新事件。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录 AWS 账户 中的事件（包括标签编辑器事件），请创建跟踪（trail）。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。默认情况下，在使用控制台创建跟踪时，此跟踪应用于所有 AWS 区域。此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Amazon S3 桶。此外，您可以配置其他AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅以下资源：

- 为您的 AWS 账户 创建跟踪
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个区域的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail 日志文件

所有标签编辑器操作均由《标签编辑器 API 参考》记录 CloudTrail 并记录在《标签编辑器 API 参考》中。控制台中的标签编辑器操作由记录并显示为事件 CloudTrail，并显示`tagging.amazonaws.com`为事件`eventSource`。

每个事件或日记账条目都包含有关生成请求的人员信息。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是 IAM 用户凭证发出的。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务 发出。

有关更多信息，请参阅CloudTrail`userIdentity`元素。

了解标签编辑器日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

以下示例显示了演示该操作的 CloudTrail 日志条目`TagResources`。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661372702",
```

```
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661372702",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-24T20:25:03Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-24T20:27:14Z",
    "eventSource": "tagging.amazonaws.com",
    "eventName": "TagResources",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.65",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resourcegroupstaggingapi.tag-resources",
    "requestParameters": {
        "resourceARNList": [
            "arn:aws:events:us-east-1:123456789012:rule/SecretsManagerMonitorRule"
        ],
        "tags": {
            "owner": "alice"
        }
    },
    "responseElements": {
        "failedResourcesMap": {}
    },
    "requestID": "8f9ea891-4125-460c-802f-26c11EXAMPLE",
    "eventID": "b2c9322a-aad7-424b-8f0b-423daEXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
```

```
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "tagging.us-east-1.amazonaws.com"
    }
}
```

标签编辑器的合规性验证

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了部署以安全性和合规性为重点 AWS 的基准环境的步骤。
- 在 Amazon Web Services 上进行HIPAA安全与合规架构 — 本白皮书描述了各公司如何使用 AWS 来创建HIPAA符合条件的应用程序。

> **Note**
>
> 并非所有 AWS 服务 人都有HIPAA资格。有关更多信息，请参阅《HIPAA合格服务参考》。

- AWS 合规资源AWS — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务 并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 这 AWS 服务 可以全面了解您的安全状态 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。

- Amazon GuardDuty — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务 检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 可以帮助您满足各种合规性要求 PCIDSS，例如满足某些合规性框架规定的入侵检测要求。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

标签编辑器的恢复能力

标签编辑器可对内部服务资源执行自动备份。这些备份不可由用户配置。备份在静态时和传输中均进行加密。标签编辑器将客户数据存储在 Amazon DynamoDB 中。

AWS全球基础设施围绕AWS 区域和可用区构建。AWS 区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

如果标签被意外删除，请联系 AWS Support 中心。

有关 AWS 区域和可用区的更多信息，请参阅 AWS 全球基础设施。

标签编辑器中的基础设施安全性

标签编辑器无法提供其他隔离服务或网络流量的方法。如果适用，请使用 AWS 特定的隔离。您可以在虚拟私有云（VPC）中使用标签编辑器 API 和控制台，这样有助于最大限度地提高隐私和基础设施安全。

您可以使用 AWS 发布的 API 调用通过网络访问标签编辑器。客户端必须支持以下内容：

- 传输层安全性协议（TLS） 我们要求使用 TSL 1.2，建议使用 TSL 1.3。
- 具有完全向前保密（PFS）的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 AWS Identity and Access Management （IAM） 主体关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service (AWS STS) 生成临时安全凭证来对请求进行签名。

标签编辑器不支持基于资源的策略。

您可以从任何网络位置调用标签编辑器 API 操作，但标签编辑器不支持基于资源的访问策略，其中可以包含基于源 IP 地址的限制。您还可以使用标签编辑器策略来控制来自特定 Amazon Virtual Private Cloud (Amazon VPC) 端点或特定 VPC 的访问。事实上，这种方法隔离了在AWS网络中仅从特定 VPC 到给定资源的网络访问。

服务限额

下表提供了有关标签编辑器的服务限额的信息。

目前无法通过服务限额控制台对这些限制进行调整。联系 AWS Support。

名称	默认
每个资源的附加标签数	50 个用户定义的标签（AWS 生成的标签不计入此限制。）
标签键名称	最少 1，UTF-8 中最多 128 个 Unicode 字符。 允许使用的字符包括字母、数字、空格以及以下字符： `_ . : / = + - @` 密钥名称不能以开头，`aws:`因为该前缀已保留供 AWS 使用。 **Note** 有些 AWS 服务 还有一些额外的字符或长度限制。有关详细信息，请参阅特定服务的文档。
标签值	最小值为 0，UTF-8 中最多 256 个 Unicode 字符。 允许使用的字符包括字母、数字、空格以及以下字符： `_ . : / = + - @`

名称	默认	
	Note 有些 AWS 服务 还有一些额外的字符或长度限制。有关详细信息，请参阅特定服务的文档。	
调用GetResourcesAPI操作的速率	每秒最多 15 次调用	
调用以下API操作的速率： • TagResources • UntagResources • GetTagKeys • GetTagValues	每秒最多 5 次调用	

标签编辑器文档历史记录

变更	说明	日期
更新了评估组织范围合规性的权限	更新了用于评估组织范围合规性的权限，以包括帮助访问合规报告的权限。	2024 年 8 月 28 日
更新的内容	更新了主题标题并重新组织了内容，以提高可读性和可发现性。	2024 年 7 月 25 日
为来自的内容添加标签 AWS 一般参考 已移至本指南	关于给你加标签的主题 AWS 资源已从 AWS 一般参考 阅读本指南。	2023 年 3 月 24 日
IAM最佳实践更新	更新了指南以符合IAM最佳实践。有关更多信息，请参阅中的安全最佳实践IAM。	2023 年 1 月 3 日
将标签编辑器文档移至其自己的指南中	标签编辑器文档现在在自己的用户指南中提供，而不是其中的一部分 AWS Resource Groups 用户指南。	2022 年 12 月 13 日
检查标签策略的合规性	在使用创建标签策略并将其附加到账户之后 AWS Organizations，你可以在组织账户中的资源上找到不合规的标签。	2019 年 11 月 26 日
标签编辑器现已支持查找未标记的资源	您现在能够在标签编辑器中搜索资源，这些资源没有适用于特定标签密钥的标签值。	2019 年 6 月 18 日
标签编辑器控制台移出 AWS Systems Manager 控制台	标签编辑器控制台现已独立于 Systems Manager 控制台。尽管您仍然可以在 Systems Manager 的左侧导航栏中找	2019 年 6 月 5 日

	到指向标签编辑器控制台的指针，但您可以直接从标签编辑器控制台左上角的下拉菜单中打开标签编辑器控制台 AWS Management Console.	
较旧的传统标签编辑器工具不再可用	提及旧版、经典版或旧版标签编辑器的内容已被删除；这些工具已在中不再可用 AWS。改用标签编辑器。	2019 年 5 月 14 日
标签编辑器现在支持在多个区域中标记资源	通过使用标签编辑器，您现在可以在多个区域中搜索和管理资源的标签，并且默认将当前区域添加到资源查询中。	2019 年 5 月 2 日
标签编辑器现在支持将查询结果导出到 CSV	您可以将 “查找要标记的资源” 页面上的查询结果导出到CSV格式化文件中。在标签编辑器查询结果中显示一个新的“区域”列。通过使用标签编辑器，您现在可以搜索特定标签键具有空值的资源。在现有的键中键入唯一的值时，将自动完成标签键值。	2019 年 4 月 2 日
标签编辑器现在支持将所有资源类型添加到查询中	您可以在单个操作中将标签应用于最多 20 种单独的资源类型，也可以选择所有资源类型以查询区域中的所有资源类型。自动完成已添加到查询的标签键字段，以帮助将标签键在资源之间保持一致。如果标签更改在某些资源上失败，您可以仅在标签更改失败的资源上重试标签更改。	2019 年 3 月 19 日

标签编辑器现在支持在搜索中使用多种资源类型	您可以在单个操作中将标签应用于最多 20 种资源类型。您也可以选择在搜索结果中向您显示的列，包括位于搜索结果中的每个唯一标签键的列或从结果中选择的资源。	2019 年 2 月 26 日

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。