aws

用户指南

AWS Resource Groups

AWS Resource Groups: 用户指南

Table of Contents

什么是资源组？

您可以使用资源组来组织 AWS 资源。 AWS Resource Groups 是一项服务，可让您同时管理和自动执行大量资源上的任务。本指南向您展示如何在 AWS Resource Groups中创建和管理资源组。您可以对资源执行的任务因所使用的 AWS 服务而异。有关支持的服务列表 AWS Resource Groups 以及每项服务允许您对资源组执行的操作的简要说明，请参阅AWS 与之配合使用的服务 AWS Resource Groups。

您可以通过以下任何入口点访问 Resource Groups。

- 在导航栏的 AWS Management Console 中，选择服务。然后，在管理和治理下，选择 Resource Groups 和标签编辑器。

  直接链接：AWS Resource Groups 控制台
- 通过在 AWS CLI 命令或 AWS SDK编程语言中使用 R API esource Groups。有关更多信息，请参阅“ AWS Resource Groups API参考”。

在 AWS Management Console 家中使用资源组

1. 登录到 AWS Management Console。
2. 在导航栏中，选择服务。
3. 在管理和治理下，选择 Resource Groups 和标签编辑器。
4. 在左侧的导航窗格中，选择保存的资源组以使用现有组，或选择创建组以创建新组。

资源及其群组类型

在中 AWS，资源是您可以使用的实体。示例包括亚马逊EC2实例、 AWS CloudFormation 堆栈或 Amazon S3 存储桶。如果您使用多个资源，您可能会发现将它们作为一个组进行管理，而不是为每项任务从一个 AWS 服务转移到另一个服务会很有用。如果您管理大量相关资源，例如构成应用程序层的EC2实例，则可能需要同时对这些资源执行批量操作。批量操作的示例包括：

- 应用更新或安全补丁。
- 升级应用程序。
- 打开或关闭到网络流量的端口。
- 从您的实例队列收集特定的日志和监控数据。

资源组是指所有 AWS 资源都相同 AWS 区域且符合组查询中指定的条件的资源集合。
在 Resource Groups 中，您可以使用两种类型的查询来建立组。两种查询类型包含使用 AWS::*service*::*resource* 格式指定的资源。

- 基于标签

  基于标签的资源组的成员资格基于指定资源类型和标签列表的查询。标签 是帮助您在组织中识别资源以及对其进行排序的键。（可选）标签包含键的值。

  > **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。

- AWS CloudFormation 基于堆栈

  AWS CloudFormation 基于堆栈的资源组的成员资格基于在当前区域中指定您账户中的 AWS CloudFormation 堆栈的查询。可在堆栈中选择要包含在组中的资源类型。您只能基于一个 AWS CloudFormation 堆栈进行查询。

服务关联资源组

有些 AWS 服务 定义的资源组只能通过使用该服务的控制台来创建和管理APIs。在 Resource Groups 控制台中，您可以对这些组执行的操作受到限制。有关更多信息，请参阅《AWS Resource Groups API参考指南》中的资源组服务配置。

可以嵌套 资源组；资源组可以包含同一区域中的现有资源组。

资源组的使用案例

默认情况下 AWS Management Console ，按 AWS 服务组织。但是使用 Resour AWS CloudFormation ce Groups，您可以创建自定义控制台，根据标签中指定的标准或堆栈中的资源来组织和整合信息。以下列表描述了资源分组可以帮助组织资源的一些情况。

- 具有不同阶段（如开发、暂存和生产）的应用程序。
- 由多个部门或个人管理的项目。
- 一组 AWS 资源，您可以一起用于公共项目，或者您想作为一个组进行管理或监视的一组资源。
- 与在特定平台（如 Android 或 iOS）上运行的应用程序相关的一组资源。

例如，您要开发一个 Web 应用程序，要为 alpha、beta 和发布阶段维护单独的资源集。每个版本都在 Amazon 上运行EC2，带有亚马逊 Elastic Block Store 存储空间。您使用 Elastic Load Balancing 管理流量并使用 Route 53 管理域。如果不使用 Resource Groups，仅仅为了检查服务的状态，或者为了修改一个应用程序版本的设置，您可能也必须访问多个控制台。

使用 Resource Groups，您可以使用单个页面查看和管理自己的资源。例如，假设您使用该工具为应用程序的每个版本（alpha、beta 和发布版）创建资源组。要检查您的应用程序的 alpha 版本的资源，请打开资源组。然后在资源组页面上查看整合信息。要修改特定资源，请选择资源组页面上的相应资源，以访问具有所需设置的服务控制台。

AWS Resource Groups 和权限

Resource Groups 功能权限为账户级别。只要共享您账户的IAM委托人（例如角色和用户）拥有正确的IAM权限，他们就可以使用您创建的资源组。

标签是资源的属性，因此它们由您的整个账户共享。部门或专门组中的用户可从公用词汇表（标签）中进行选择，以创建对自己的角色和职责有意义的资源组。采用公用标签池还意味着用户在共享资源组时，不必担心标签信息缺失或冲突。

AWS Resource Groups 资源

在 Resource Groups 中，唯一可用的资源是组。群组具有与其关联的唯一 Amazon 资源名称 (ARNs)。有关更多信息ARNs，请参阅中的 Amazon 资源名称 (ARN) 和 AWS 服务命名空间。Amazon Web Services 一般参考

资源类型	ARN格式
资源组	`arn:aws:resource-groups:` *`region`*`:`*`account`*`:group/`*`group-name`

标记的工作原理

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，无论是 Amazon EC2 实例、Amazon S3 存储桶还是其他资源，您都可以在创建资源时选择添加标签。不过，您也可以使用标签编辑器一次向多个受支持资源添加标签。您针对各个类型的资源构建查询，然后为搜索结果中的资源添加、删除或替换标签。基于标签的查询将 AND 运算符分配给标签，以便查询返回与指定资源类型和所有指定的标签匹配的任何资源。

> **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。

有关更多信息，请参阅标签编辑器用户指南。您可以使用标签编辑器标记支持的资源，并在创建和管理资源的服务控制台中使用标记功能标记一些其他资源。

入门 AWS Resource Groups

在中 AWS，资源是您可以使用的实体。示例包括亚马逊EC2实例、亚马逊 S3 存储桶或亚马逊 Route 53 托管区域。如果您使用多个资源，您可能会发现将它们作为一个组进行管理，而不是为每项任务从一个 AWS 服务转移到另一个服务会很有用。

本节向您展示如何开始使用 AWS Resource Groups。首先，通过在标签编辑器中为 AWS 资源添加标签来组织资源。然后，在 Resource Groups 中构建查询，其中包括组中所需的资源类型，以及已应用于资源的标签。

在 Resource Groups 中创建资源组后，使用诸如自动化之类的 AWS Systems Manager 工具来简化资源组的管理任务。

有关 AWS Systems Manager 功能和工具入门的更多信息，请参阅《AWS Systems Manager 用户指南》。

主题

- 使用的先决条件 AWS Resource Groups
- 了解有关 AWS Resource Groups 授权和访问控制的更多信息

使用的先决条件 AWS Resource Groups

在开始使用资源组之前，请确保您的资源组处于活动状态 AWS 具有现有资源和适当权限的帐户，可以标记资源和创建群组。

主题

- 报名参加 AWS
- 创建资源

- 设置权限

报名参加 AWS

如果你没有 AWS 账户，请完成以下步骤来创建一个。

要注册 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。

创建资源

您可以创建空的资源组，但在组中有资源之前，您无法对资源组成员执行任何任务。有关支持的资源类型的更多信息，请参阅可以与标签编辑器一起 AWS Resource Groups 使用的资源类型。

设置权限

要充分利用资源组和标签编辑器，您可能需要更多权限来标记资源或查看资源的标签键和值。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
- 使用所需的权限 AWS Resource Groups 控制台和API。

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。您首先创建委托人，例如IAM角色或用户，或者将外部身份与您的用户相关联 AWS 使用诸如此类的服务的环境 AWS IAM Identity Center。 然后，您可以应用具有用户所需权限的策略。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**
>
> 本节介绍在您想要标记来自其他服务控制台的资源并将APIs这些资源添加到资源组时所需的权限。

如资源及其群组类型中所述，每个资源组都表示共享一个或多个标签键或值的指定类型的资源的集合。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中执行标记操作的权限API，例如《亚马逊EC2用户指南》中列出的那些操作。

要充分利用资源组功能，您需要允许访问服务控制台以及在其中与资源进行交互的其他权限。有关亚马逊此类政策的示例EC2，请参阅《亚马逊EC2用户指南》中的亚马逊EC2控制台操作策略示例。

Resource Groups 和标签编辑器所需的权限

要使用 Resource Groups 和标签编辑器，必须将以下权限添加到中的用户策略声明中IAM。你可以添加任一项 AWS-由维护和保存 up-to-date 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 Resource Groups 和标签编辑器权限的托管策略

AWS Resource Groups 标签编辑器支持以下内容 AWS 托管策略，可用于向用户提供一组预定义的权限。您可以将这些托管策略附加到任何用户、角色或组，就像您创建的任何其他策略一样。

ResourceGroupsandTagEditorReadOnlyAccess

此策略向附加的IAM角色或用户授予对 Resource Groups 和标签编辑器调用只读操作的权限。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（请参阅以下“重要说明”）。

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（请参阅以下“重要说明”）。

Important

前两项策略授予调用 Resource Groups 和标签编辑器操作以及使用这些控制台的权限。对于 Resource Groups 操作，这些策略已足够，并且会授予在资源组控制台中使用任何资源所需的所有权限。
但是，对于标记操作和标签编辑器控制台，权限更加精细。您不仅必须拥有调用该操作的权限，还必须拥有对您尝试访问其标签的特定资源的相应权限。要授予标签的访问权限，您还必须附加以下策略之一：

- 这些区域有： AWS-managed 策略ReadOnlyAccess授予每个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 可用时提供的服务。
- 许多服务都提供特定于服务的只读模式 AWS-托管策略，可用于限制仅访问该服务提供的资源。例如，亚马逊EC2提供亚马逊EC2ReadOnlyAccess。
- 您可以创建自己的策略，仅针对您希望用户访问的少数服务和资源授予非常具体的只读操作访问权限。此策略使用“允许列表”策略或拒绝列表策略。

  允许列表策略利用这样一个事实，即在策略中明确允许访问之前，默认情况下会拒绝访问。您可以使用以下示例的策略：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [ "resource-groups:*" ],
            "Resource": "arn:aws:resource-groups:*:123456789012:group/*"
        }
    ]
}
```

  或者，您可以使用“拒绝列表”策略，即允许访问除您明确阻止的资源之外的所有资源。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
             "Action": [ "resource-groups:*" ],
            "Resource": "arn:aws:resource-groups:*:123456789012:group/*"
        }
```

```
    ]
}
```

手动添加 Resource Groups 和标签编辑器权限

- `resource-groups:*`（此权限允许执行所有 Resource Groups 操作。 如果您想限制用户可用的操作，则可以将星号替换为特定的 Resource Groups 操作，或者替换为以逗号分隔的操作列表）
- `cloudformation:DescribeStacks`
- `cloudformation:ListStackResources`
- `tag:GetResources`
- `tag:TagResources`
- `tag:UntagResources`
- `tag:getTagKeys`
- `tag:getTagValues`
- `resource-explorer:*`

> **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。

要在控制台中使用 Resource Groups 和标签编辑器，还需要运行 `resource-groups:ListGroupResources` 操作的权限。此权限是列出当前区域中可用资源类型所必需的条件。当前不支持使用带 `resource-groups:ListGroupResources` 的策略条件。

授予使用权限 AWS Resource Groups 和标签编辑器

添加策略以供使用 AWS Resource Groups 然后对用户使用标签编辑器，请执行以下操作。

1. 打开控制IAM台。
2. 在导航窗格中，选择用户。

3. 找到您要向其授予权限的用户 AWS Resource Groups 和标签编辑器权限。选择用户的名称以打开用户属性页。
4. 选择 Add permissions（添加权限）。
5. 选择 Attach existing policies directly（直接附上现有策略）。
6. 选择创建策略。
7. 在JSON选项卡上，粘贴以下政策声明。

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

> **Note**
>
> 此示例策略声明仅授予以下各项的权限 AWS Resource Groups 和标签编辑器操作。它不允许访问 AWS Systems Manager 中的任务 AWS Resource Groups console。例如，此策略不授予您使用 Systems Manager 自动化命令的权限。要对资源组执行 Systems Manager 任务，您必须将 Systems Manager 权限附加到您的策略（例如 `ssm:*`）。有关授予对 Systems Manager 访问权限的更多信息，请参阅《配置对 Systems Manager 的访问权限》AWS Systems Manager 用户指南。

8. 选择查看策略。
9. 为新策略指定名称和描述（例如 `AWSResourceGroupsQueryAPIAccess`）。

10. 选择创建策略。
11. 现在，策略已保存在中IAM，您可以将其附加到其他用户。有关如何向用户添加策略的更多信息，请参阅《用户指南》中的通过将策略直接附加到用户来添加权限。IAM

了解有关 AWS Resource Groups 授权和访问控制的更多信息

Resource Groups 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 ListGroups 操作，但不能执行其他操作。
- 资源级权限。Resource G ARNsroups 支持使用来指定策略中的单个资源。
- 根据标签进行授权。Resource Groups 支持在策略条件下使用资源标签。例如，您可以创建一个策略，以允许 Resource Groups 用户对您已标记的组具有完全访问权限。
- 临时凭证。用户可以通过允许 AWS Resource Groups 操作的策略来扮演角色。

Resource Groups 不支持基于资源的策略。

有关 Resource Groups 和标签编辑器如何与 AWS Identity and Access Management (IAM) 集成的更多信息，请参阅AWS Identity and Access Management 用户指南中的以下主题。

- AWS 与之配合使用的服务 IAM
- 的操作、资源和条件键 AWS Resource Groups
- 使用策略控制访问

AWS 与之配合使用的服务 AWS Resource Groups

您可以将以下 AWS 服务与一起使用 AWS Resource Groups。

AWS 服务	与 Resource Groups 结合使用
AWS CloudFormation— 使用堆栈模板 AWS CloudFormation 在中创建资源组。	同时提供和组织 AWS 资源。按标签整理资源。整理其他堆栈中的资源。使用 Amazon 在 AWS 资源组中收集有关您的资源的见解，CloudWatch 或者使用采取运营措施 AWS Systems Manager。

AWS 服务	与 Resource Groups 结合使用
	有关更多信息，请参阅《AWS CloudFormation 用户指南》中的ResourceGroups资源类型参考。
CloudTrail— 使用捕获所有资源组操作 AWS CloudTrail。	捕获有关对您的资源组执行的操作的信息，包括执行操作的人员（IAM 委托人，例如角色、用户或 AWS 服务）、何时执行操作、操作发生在何处（源 IP 地址）等详细信息。然后，这些记录可用于分析或触发后续操作。 有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。
Amazon CloudWatch — 启用对您的 AWS 资源和您运行的应用程序的实时监控 AWS。	您可以将视图专注于显示单个资源组中的指标和告警。 有关更多信息，请参阅 Amazon CloudWatch 用户指南中的关注资源组中的指标和警报。
Amazon CloudWatch 应用程序见解 — 检测基于.NET 和 SQL Server 的应用程序的常见问题。	监控属于资源组的 .NET 和 SQL Server 应用程序资源。 有关更多信息，请参阅 Amazon CloudWatch 用户指南中的支持的应用程序组件。
Amazon DynamoDB 表组 – 将您的 DynamoDB 表整理成逻辑分组，以便更轻松地管理资源。	在 DynamoDB 操作菜单中创建、编辑和删除一组 DynamoDB 表。 有关更多信息，请参阅 Amazon DynamoDB 开发人员指南。
Amazon EC2 专属主机 – 使用按插槽、按内核或按虚拟机授权的现有软件许可证，包括 Windows Server、Microsoft SQL Server、SUSE 和 Linux Enterprise Server。	将 Amazon EC2 实例启动到主机资源组中，以帮助最大限度地提高专属主机的利用率。 有关更多信息，请参阅 Amazon EC2 用户指南中的使用专用主机。

AWS 服务	与 Resource Groups 结合使用
Amazon EC2 容量预留 – 为您的 Amazon EC2 实例预留容量，以便在需要时使用。您可以为容量预留指定属性，使其仅适用于使用匹配属性启动的 Amazon EC2 实例。	将您的 Amazon EC2 实例启动到包含一个或多个容量预留的资源组中。如果该组没有具有匹配属性和所请求实例可用容量的容量预留，则该实例将作为按需实例运行。如果稍后将匹配的容量预留添加到目标组中，则实例将自动与其预留容量匹配并移动到该容量中。 有关更多信息，请参阅 Amazon EC2 用户指南中的使用容量预留组。
AWS License Manager – 简化将软件供应商许可证迁移到云的过程。	配置主机资源组以允许 License Manager 管理您的专属主机。 有关更多信息，请参阅 License Manager 用户指南中的 License Manager 中的主机资源组。
AWS 弹性中心 — 准备并保护您的应用程序免受中断。	发现使用 Resource Groups 定义的应用程序。 有关更多信息，请参阅 AWS 新闻博客中的使用 AWS Resilience Hub 衡量和提高您的应用程序弹性。
AWS Resource Access Manager— 与其他账户共享您拥有的指定 AWS 资源。	使用共享主机资源组 AWS RAM。 有关更多信息，请参阅 AWS RAM 用户指南中的可共享的资源。
AWS Service Catalog AppRegistry – 定义和管理您的应用程序及其元数据。	当您在中创建应用程序时 AppRegistry，该服务会自动为该应用程序创建资源组。应用程序资源组是应用程序中所有资源的集合。该服务还会为与 AWS CloudFormation 应用程序关联的每个堆栈创建一个基于堆栈的资源组。 有关更多信息，请参阅《AWS Service Catalog 管理员指南》 AppRegistry中的 “使用”。

AWS 服务	与 Resource Groups 结合使用
AWS Systems Manager— 启用 AWS 资源的可见性和控制力。	收集运营见解，并根据资源组对应用程序采取批量操作。在 AWS Systems Manager 控制台中，Application Manager 的 “自定义应用程序” 页面会自动导入并显示基于资源组的应用程序的操作数据。您可以使用 Application Manager 上的信息来帮助您确定组中的哪些资源符合要求并且正常工作，以及哪些资源需要操作。 有关更多信息，请参阅 AWS Systems Manager 用户指南中的在 Application Manager 中使用应用程序。
Amazon VPC 网络访问分析器 – 可识别对 AWS 上资源的不必要网络访问。	您可以使用来指定网络访问要求的来源和目的地 AWS Resource Groups。这使您可以管理整个 AWS 环境中的网络访问权限，而无需考虑如何配置网络。 有关更多信息，请参阅 Amazon 虚拟私有云用户指南中的将 Resource Groups 与 网络访问范围结合使用。

资源组的服务配置

资源组使您可以将 AWS 资源集合作为一个单元进行管理。某些 AWS 服务通过对组的所有成员执行所请求操作来支持这一点。此类服务可以将应用于群组成员的设置存储为附加到群组JSON的数据结构形式的配置。

本主题介绍所支持 AWS 服务的可用配置设置。

主题

- 如何访问附加到资源组的服务配置
- JSON服务配置的语法
- 支持的配置类型和参数

如何访问附加到资源组的服务配置

支持服务关联组的服务通常会在您使用该服务提供的工具（例如该服务的管理控制台或其 AWS CLI 和 AWS SDK操作）时为您设置配置。某些服务会完全管理其服务相关组，除非控制台允许或所属 AWS 服务提供的命令，否则您无法以任何方式对其进行修改。但是，在某些情况下，您可以使用以下API操作 AWS SDKs或其 AWS CLI 等效操作与服务配置进行交互：

- 使用CreateGroup操作创建群组时，您可以将自己的配置附加到群组。
- 您可以使用PutGroupConfiguration操作修改附加到组的当前配置。
- 您可以通过调用GetGroupConfiguration操作来查看资源组的当前配置。

JSON服务配置的语法

资源组可以包含一种配置，该配置定义适用于作为该组成员的资源的服务特定设置。

配置以JSON对象的形式表示。在最顶层，配置是组配置项目的数组。每个组配置项目都包含两个元素：用于配置的 `Type`，以及由该类型定义的一组 `Parameters`。每个参数都包含一个 `Name` 和一个或多个 `Values` 的数组。下面的例子是 *`placeholders`* 显示了单个示例资源类型配置的基本语法。此示例显示了具有两个参数的类型，并且每个参数都有两个值。下一节将讨论实际有效的类型、参数和值。

```
[
    {
        "Type": "configuration-type",
        "Parameters": [
            {
                "Name": "parameter1-name",
                "Values": [
                    "value1",
                    "value2"
                ]
            },
            {
                "Name": "parameter2-name",
                "Values": [
                    "value3",
                    "value4"
                ]
            }
        ]
    }
```

```
]
```

支持的配置类型和参数

资源组支持使用以下配置类型。每种配置类型都有一组对该类型有效的参数。

主题

AWS::ResourceGroups::Generic

此配置类型指定对资源组强制成员资格要求的设置，而不是为 AWS 服务配置特定资源类型的行为。此配置类型由需要它的服务关联组自动添加，例如 AWS::EC2::CapacityReservationPool 和 AWS::EC2::HostManagment 类型。

以下 Parameters 对AWS::ResourceGroups::Generic服务关联组Type有效。

- **allowed-resource-types**

  此参数指定资源组只能由一个或多个指定类型的资源组成。

  值的数据类型：字符串

  允许的值：

  - AWS::EC2::Host– 当服务配置还包含类型 AWS::EC2::HostManagement 的 Configuration 时，需要使用带有此参数和值的 Configuration。这样可以确保该HostManagement群组只能包含 Amazon EC2 专用主机。
  - AWS::EC2::CapacityReservation– 当服务配置还包含类型 AWS::EC2::CapacityReservationPool 的 Configuration 项目时，需要使用带有此参数和值的 Configuration。这样可以确保一个CapacityReservation组只能包含 Amazon EC2 容量预留容量。

必需：有条件，基于附加到资源组的其他 Configuration 元素。有关允许的值，请参阅前面的条目。

以下示例将群组成员限制为只有 Amazon EC2 主机实例。

```
[
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": ["AWS::EC2::Host"]
            }
        ]
    }
]
```

- **deletion-protection**

  此参数指定除非资源组不包含任何成员，否则无法将其删除。有关更多信息，请参阅 License Manager 用户指南中的删除主机资源组。

  值的数据类型：字符串数组

  允许的值：唯一允许的值是 ["UNLESS_EMPTY"]（该值必须为大写）。

  必需：有条件，基于附加到资源组的其他 Configuration 元素。仅当资源组还有另一个带有 Type 的 AWS::EC2::HostManagement 的 Configuration 元素时，才需要此参数。

  以下示例为该组启用删除保护，除非该组没有成员才能将其删除。

```
[
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "deletion-protection",
                "Values": [ "UNLESS_EMPTY" ]
            }
        ]
    }
```

```
]
```

AWS::AppRegistry::Application

此Configuration类型指定资源组代表由创建的应用程序 AWS Service Catalog AppRegistry。

此类资源组完全由 AppRegistry 服务管理，只有使用提供的工具才能由用户创建、更新或删除 AppRegistry。

> **Note**
>
> 由于此类资源组由 AWS 用户自动创建和维护，而不是由用户管理，因此这些资源组不计入您在中可以创建的最大资源组数量的配额限制 AWS 账户。

有关更多信息，请参阅《S ervice Catalog 用户指南》 AppRegistry中的 “使用”。

在 AppRegistry 创建此类服务相关资源组时，它还会自动为AWS CloudFormation 与应用程序关联的每个 AWS CloudFormation 堆栈创建一个单独的附加服务相关组。

AppRegistry 使用前缀AWS_AppRegistry_Application-和应用程序名称自动命名其创建的此类服务相关组：AWS_AppRegistry_Application-*MyAppName*

AWS::AppRegistry::Application 服务关联组类型支持以下参数。

- **Name**

  此参数指定在中创建应用程序时由用户分配的友好名称 AppRegistry。

  值的数据类型：字符串

  允许的值： AppRegistry 服务允许的应用程序名称的任何文本字符串。

  必需：是

- **Arn**

  此参数指定由分配的应用程序的 Amazon 资源名称 (ARN) 路径 AppRegistry。

  值的数据类型：字符串

允许的值：有效ARN。

必需：是

> **Note**
>
> 要更改这些元素中的任何一个，必须使用 AppRegistry 控制台或该 AWS SDK服务和 AWS CLI 操作来修改应用程序。

此应用程序资源组自动将为与 AppRegistry 应用程序关联的AWS CloudFormation 堆栈创建的资源组列为组成员。您可以使用该ListGroupResources操作来查看这些子组。

以下示例显示了 `AWS::AppRegistry::Application` 服务关联组的配置部分。

```
[
    {
        "Type": "AWS::AppRegistry::Application",
        "Parameters":[
            {
                "Name": "Name",
                "Values": [
                    "MyApplication"
                ]
            },
            {
                "Name": "Arn",
                "Values": [
                    "arn:aws:servicecatalog:us-east-1:123456789012:/
applications/<application-id>"
                ]
            }
        ]
    }
]
```

AWS::CloudFormation::Stack

此Configuration类型指定组代表 AWS CloudFormation 堆栈，其成员是该堆栈创建的 AWS 资源。

当您将 AWS CloudFormation 堆栈与 AppRegistry 服务关联时，系统会自动为您创建此类资源组。除非使用提供的工具，否则您无法创建、更新或删除这些群组 AppRegistry。

AppRegistry 使用前缀`AWS_CloudFormation_Stack-`和堆栈名称自动命名其创建的此类服务相关组：`AWS_CloudFormation_Stack-`*`MyStackName`*

> **Note**
>
> 由于此类资源组由 AWS 用户自动创建和维护，而不是由用户管理，因此这些资源组不计入您在中可以创建的最大资源组数量的配额限制 AWS 账户。

有关更多信息，请参阅《S ervice Catalog 用户指南》 AppRegistry中的 “使用”。

AppRegistry 自动为您与 AppRegistry 应用程序关联的每个 AWS CloudFormation 堆栈创建此类服务相关资源组。这些资源组将成为 AppRegistry应用程序父资源组的子成员。

该 AWS CloudFormation 资源组的成员是作为堆栈的一部分创建的 AWS 资源。

`AWS::CloudFormation::Stack` 服务关联组类型支持以下参数。

- **`Name`**

  此参数指定创建 AWS CloudFormation 堆栈时用户分配的堆栈的友好名称。

  值的数据类型：字符串

  允许的值： AWS CloudFormation 服务允许的堆栈名称的任何文本字符串。

  必需：是

- **`Arn`**

  此参数指定附加到中应用程序的 AWS CloudFormation 堆栈的 Amazon 资源名称 (ARN) 路径 AppRegistry。

  值的数据类型：字符串

  允许的值：有效ARN。

  必需：是

> **Note**
>
> 要更改这些元素中的任何一个，必须使用 AppRegistry 控制台或等效工具 AWS SDK和 AWS CLI 操作来修改应用程序。

以下示例显示了 AWS::CloudFormation::Stack 服务关联组的配置部分。

```
[
    {
        "Type": "AWS::CloudFormation::Stack",
        "Parameters":[
            {
                "Name": "Name",
                "Values": [
                    "MyStack"
                ]
            },
            {
                "Name": "Arn",
                "Values": [
                    "arn:aws:cloudformation:us-
east-1:123456789012:stack/MyStack/<stack-id>"
                ]
            }
        ]
    }
]
```

AWS::EC2::CapacityReservationPool

此 Configuration 类型指定资源组表示该组成员提供的公共容量池。该资源组的成员必须是 Amazon EC2 容量预留人员。资源组可以包括您在账户中拥有的容量预留以及通过使用从其他账户与您共享的容量预留 AWS Resource Access Manager。这允许您使用此资源组作为容量预留参数的值来启动 Amazon EC2 实例。当您执行此操作时，实例将使用组中的可用预留容量。如果资源组没有可用容量，则该实例将作为池外部的独立按需实例启动。有关更多信息，请参阅 Amazon EC2 用户指南中的使用容量预留组。

如果您使用此类型的 Configuration 项目配置服务关联资源组，则还必须使用以下值指定单独的 Configuration 项目：

- 具有一个参数的 AWS::ResourceGroups::Generic 类型：
  - 参数 allowed-resource-types 和单个值 AWS::EC2::CapacityReservation。这样可以确保只有 Amazon EC2 容量预留可以成为资源组的成员。

组配置中的 AWS::EC2::CapacityReservationPool 项目不支持任何参数。

以下示例展示此类组的 Configuration 部分。

```
[
    {
        "Type": "AWS::EC2::CapacityReservationPool"
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": [ "AWS::EC2::CapacityReservation" ]
            }
        ]
    }
]
```

AWS::EC2::HostManagement

此标识符指定了 Amazon EC2 主机管理的设置 AWS License Manager ，这些设置是针对群组成员强制执行的。有关更多信息，请参阅中的主机资源组 AWS License Manager。

如果您使用此类型的 Configuration 项目配置服务关联资源组，则还必须使用以下值指定单独的 Configuration 项目：

- 一种 AWS::ResourceGroups::Generic 类型，其参数为 allowed-resource-types，单个值为 AWS::EC2::Host。这样可以确保只有 Amazon EC2 专用主机可以成为该群组的成员。
- 一种 AWS::ResourceGroups::Generic 类型，其参数为 deletion-protection，单个值为 UNLESS_EMPTY。这样可以确保除非组为空，否则无法删除该组。

AWS::EC2::HostManagement 服务关联组类型支持以下参数。

- **auto-allocate-host**

此参数指定实例是在特定的专属主机上启动，还是在具有匹配配置的任何可用主机上启动。有关更多信息，请参阅《A mazon EC2 用户指南》中的 “了解自动投放和亲和力”。

值的数据类型：布尔值

允许的值：“true”或“false”（必须为小写）。

必需：否

```
[
    {
        "Type": "AWS::EC2::HostManagement",
        "Parameters": [
            {
                "Name": "auto-allocate-host",
                "Values": [ "true" ]
            },
            {
                "Name": "any-host-based-license-configuration",
                "Values": ["true"]
            }
        ]
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": [ "AWS::EC2::Host" ]
            },
            {
                "Name": "deletion-protection",
                "Values": [ "UNLESS_EMPTY" ]
            }
        ]
    }
]
```

- **auto-release-host**

  此参数指定组中的专属主机在上次运行的实例终止后是否自动释放。有关更多信息，请参阅 Amazon EC2 用户指南中的释放专用主机。

值的数据类型：布尔值

允许的值：“true”或“false”（必须为小写）。

必需：否

```
[
    {
        "Type": "AWS::EC2::HostManagement",
        "Parameters": [
            {
                "Name": "auto-release-host",
                "Values": [ "false" ]
            },
            {
                "Name": "any-host-based-license-configuration",
                "Values": ["true"]
            }
        ]
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": [ "AWS::EC2::Host" ]
            },
            {
                "Name": "deletion-protection",
                "Values": [ "UNLESS_EMPTY" ]
            }
        ]
    }
]
```

- **allowed-host-families**

  此参数指定属于该组的实例可以使用哪些实例类型系列。

  值的数据类型：字符串数组。

允许的值：每个值都必须是有效的 Amazon EC2 实例类型系列标识符C4，例如M5P3dn、、或R5d。

必需：否

以下示例配置项目指定启动的实例只能是 C5 或 M5 实例类型系列的成员。

```
[
    {
        "Type": "AWS::EC2::HostManagement",
        "Parameters": [
            {
                "Name": "allowed-host-families",
                "Values": ["c5", "m5"]
            },
            {
                "Name": "any-host-based-license-configuration",
                "Values": ["true"]
            }
        ]
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": ["AWS::EC2::Host"]
            },
            {
                "Name": "deletion-protection",
                "Values": ["UNLESS_EMPTY"]
            }
        ]
    }
]
```

- **allowed-host-based-license-configurations**

  此参数指定要应用于群组成员的一个或多个基于内核/套接字的许可配置的 Amazon 资源名称 (ARN) 路径。

  值的数据类型：数组ARNs。

允许的值：每个值都必须是有效的 L icense Manager 配置ARN。

必填：条件性。您可以指定此参数或 any-host-based-license-configuration，但不能同时指定两者。这些参数是互斥的。

以下示例配置项指定组成员可以使用两个指定的 License Manager 配置。

```
[
    {
        "Type": "AWS::EC2::HostManagement",
        "Parameters": [
            {
                "Name": "allowed-host-based-license-configurations",
                "Values": [
                    "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-6eb6586f508a786a2ba41EXAMPLE1111",
                    "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-8a786a26f50ba416eb658EXAMPLE2222"
                ]
            }
        ]
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": [ "AWS::EC2::Host" ]
            },
            {
                "Name": "deletion-protection",
                "Values": [ "UNLESS_EMPTY" ]
            }
        ]
    }
]
```

- **any-host-based-license-configuration**

  此参数指定您不想将特定的许可证配置关联到您的组。在这种情况下，所有基于内核/套接字的许可证配置都可供主机资源组中的成员使用。如果您的许可证数量不限，并且想要针对主机利用率进行优化，请使用此设置。

值的数据类型：布尔值

允许的值：“true”或“false”（必须为小写）。

必填：条件性。您可以指定此参数或 allowed-host-based-license-configurations，但不能同时指定两者。这些参数是互斥的。

以下示例配置项指定组成员可以使用任何基于内核/套接字的许可证配置。

```
[
    {
        "Type": "AWS::EC2::HostManagement",
        "Parameters": [
            {
                "Name": "any-host-based-license-configuration",
                "Values": ["true"]
            }
        ]
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": ["AWS::EC2::Host"]
            },
            {
                "Name": "deletion-protection",
                "Values": ["UNLESS_EMPTY"]
            }
        ]
    }
]
```

以下示例说明如何将所有主机管理设置一起包含在单个配置中。

```
[
    {
        "Type": "AWS::EC2::HostManagement",
        "Parameters": [
            {
```

```
                "Name": "auto-allocate-host",
                "Values": ["true"]
            },
            {
                "Name": "auto-release-host",
                "Values": ["false"]
            },
            {
                "Name": "allowed-host-families",
                "Values": ["c5", "m5"]
            },
            {
                "Name": "allowed-host-based-license-configurations",
                "Values": [
                    "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-6eb6586f508a786a2ba41EXAMPLE1111",
                    "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-8a786a26f50ba416eb658EXAMPLE2222"
                ]
            }
        ]
    },
    {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
            {
                "Name": "allowed-resource-types",
                "Values": ["AWS::EC2::Host"]
            },
            {
                "Name": "deletion-protection",
                "Values": ["UNLESS_EMPTY"]
            }
        ]
    }
]
```

AWS::NetworkFirewall::RuleGroup

此标识符指定对群组成员强制执行的 AWS Network Firewall 规则组的设置。防火墙管理员可以指定此类资源组的，以根据防火墙规则自动解析该组成员的 IP 地址，而不必手动列出每个地址。ARN有关更多信息，请参阅在 AWS Network Firewall中使用基于标签的资源组。

您可以使用 Network Firewall 控制台或运行 AWS CLI 命令或 AWS SDK操作来创建此配置类型的资源组。

此配置类型的资源组具有以下限制：

- 该组的成员仅由 Network Firewall 支持的资源类型组成。
- 该组必须包含基于标签的查询才能管理组的成员资格；任何支持类型的资源，如果其标签与查询相匹配，都将自动成为该组的成员。
- 此配置类型不支持 `Parameters`。
- 要删除此配置类型的资源组，任何 Network Firewall 规则组都无法引用该资源组。

以下示例说明了此类型组的 `Configuration` 和 `ResourceQuery` 部分。

```
{
    "Configuration": [
        {
            "Type": "AWS::NetworkFirewall::RuleGroup",
            "Parameters": []
        }
    ],
    "ResourceQuery": {
        "Query": "{\"ResourceTypeFilters\":[\"AWS::EC2::Instance\"],\"TagFilters\":
[{\"Key\":\"environment\",\"Values\":[\"production\"]}]}",
        "Type": "TAG_FILTERS_1_0"
    }
}
```

以下示例 AWS CLI 命令使用先前的配置和查询创建资源组。

```
$ aws resource-groups create-group \
    --name test-group \
    --resource-query '{"Type": "TAG_FILTERS_1_0", "Query": "{\"ResourceTypeFilters\":
 [\"AWS::EC2::Instance\"], \"TagFilters\": [{\"Key\": \"environment\", \"Values\":
 [\"production\"]}]}"}' \
    --configuration '[{"Type": "AWS::NetworkFirewall::RuleGroup", "Parameters": []}]'
{
    "Group":{
        "GroupArn":"arn:aws:resource-groups:us-west-2:123456789012:group/test-group",
        "Name":"test-group",
        "OwnerId":"123456789012"
```

```
    },
    "Configuration": [
        {
            "Type": "AWS::NetworkFirewall::RuleGroup",
            "Parameters": []
        }
    ],
    "ResourceQuery": {
        "Query": "{\"ResourceTypeFilters\":[\"AWS::EC2::Instance\"],\"TagFilters\":
[{\"Key\":\"environment\",\"Values\":[\"production\"]}]}",
        "Type": "TAG_FILTERS_1_0"
    }
}
```

在中创建基于查询的群组 AWS Resource Groups

资源组查询的类型

在中 AWS Resource Groups，查询是基于查询的群组的基础。您可以将资源组基于两种类型的查询之一。

基于标签

基于标签的查询包含使用以下格式 AWS::*service*::*resource* 和标签指定的资源类型列表。标签 是帮助识别组织中的资源以及对其进行排序的键。（可选）标签包含键的值。

对于基于标签的查询，您还可以指定要作为组成员的资源共享的标签。例如，如果您要创建一个资源组，其中包含用于运行应用程序测试阶段的所有 Amazon EC2 实例和 Amazon S3 存储桶，并且您的实例和存储桶以这种方式标记，请从下拉列表中选择AWS::EC2::Instance和AWS::S3::Bucket资源类型，然后指定标签密钥**Stage**，标签值为。**Test**

基于标签的资源组的 ResourceQuery 参数语法包含以下元素：

- Type

  此元素表示哪种查询定义此资源组。要创建基于标签的资源组，请按如下方式指定值 TAG_FILTERS_1_0：

  ```
  "Type": "TAG_FILTERS_1_0"
  ```

- Query

  此元素定义用于匹配资源的实际查询。它包含具有以下元素的JSON结构的字符串表示形式：

  - ResourceTypeFilters

    此元素将结果限制为仅匹配筛选条件的资源类型。可以指定以下值：

    - "AWS::AllSupported" – 指定结果可以包括与查询匹配且当前由 Resource Groups 服务支持的任意类型资源。
    - "AWS::*service-id*::*resource-type* – 以逗号分隔的资源类型规范字符串列表，其格式为：，例如 "AWS::EC2::Instance"。

  - TagFilters

此元素指定与附加到您资源的标签进行比较的键/值字符串对。标签键和值与筛选条件相匹配的内容将包含在组中。每个筛选条件都由以下元素组成：

- "Key" – 带有键名称的字符串。仅限其标签具有匹配键名称的资源与筛选条件匹配，并且是该组的成员。
- "Values" – 一个字符串，其中包含以逗号分隔的指定键值列表。仅限具有匹配标签键和值（与此列表中的一个元素匹配）是该组的成员。

所有这些JSON元素都必须组合成JSON结构的单行字符串表示形式。例如，假设Query具有以下示例JSON结构的 a。此查询仅匹配标签为 “Stage” 且值为 “Test” 的 Amazon EC2 实例。

```
{
    "ResourceTypeFilters": [ "AWS::EC2::Instance" ],
    "TagFilters": [
        {
            "Key": "Stage",
            "Values": [ "Test" ]
        }
    ]
}
```

它JSON可以表示为以下单行字符串，并用作Query元素的值。由于JSON结构的值必须是双引号字符串，因此必须对任何嵌入的双引号字符或正斜杠字符进行转义，方法是在每个字符前面加上反斜杠，如下所示：

```
"Query":"{\"ResourceTypeFilters\":[\"AWS::AllSupported\"],\"TagFilters\":[{\"Key\":
\"Stage\",\"Values\":[\"Test\"]}]}"
```

然后将完整的ResourceQuery字符串表示为CLI命令参数，如下所示：

```
--resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters\":
[\"AWS::AllSupported\"],\"TagFilters\":[{\"Key\":\"Stage\",\"Values\":[\"Test
\"]}]}"}'
```

基于AWS CloudFormation 堆栈

在 AWS CloudFormation 基于堆 AWS CloudFormation 栈的查询中，您在当前区域的账户中选择一个堆栈，然后在堆栈中选择要加入该组的资源类型。您只能基于一个 AWS CloudFormation 堆栈进行查询。

> **Note**
>
> 一个 AWS CloudFormation 堆栈可以包含其他 AWS CloudFormation “子” 堆栈。但是，基于“父”堆栈的资源组并不能将子堆栈的所有资源都作为组成员获取。资源组将子堆栈作为单个组成员添加到父堆栈的资源组中，并且不会对其进行扩展。

Resource Groups 支持基于具有以下状态之一的 AWS CloudFormation 堆栈的查询。

- `CREATE_COMPLETE`
- `CREATE_IN_PROGRESS`
- `DELETE_FAILED`
- `DELETE_IN_PROGRESS`
- `REVIEW_IN_PROGRESS`

> **Important**
>
> 只有在查询中作为堆栈一部分直接创建的资源才会包含在资源组中。以后由 AWS CloudFormation 堆栈成员创建的资源不会成为该组的成员。例如，如果由创建的自动缩放组 AWS CloudFormation 作为堆栈的一部分，则该自动缩放组就是该组的成员。但是，由该自动扩展组作为其操作一部分创建的 Amazon EC2 实例不是基于 AWS CloudFormation 堆栈的资源组的成员。

如果您基于 AWS CloudFormation 堆栈创建群组，并且该堆栈的状态更改为不再支持作为群组查询基础的群组（例如）`DELETE_COMPLETE`，则该资源组仍然存在，但它没有成员资源。

在创建资源组后，您可以在该组中的资源上执行任务。

CloudFormation 基于堆栈的资源组的`ResourceQuery`参数语法包含以下元素：

- `Type`

  此元素表示哪种查询定义此资源组。

  要创建 AWS CloudFormation 基于堆栈的资源组，请按如下方式指定值`CLOUDFORMATION_STACK_1_0`：

```
"Type": "CLOUDFORMATION_STACK_1_0"
```

- `Query`

  此元素定义用于匹配资源的实际查询。它包含具有以下元素的JSON结构的字符串表示形式：

  - `ResourceTypeFilters`

    此元素将结果限制为仅匹配筛选条件的资源类型。可以指定以下值：

    - `"AWS::AllSupported"` – 指定结果可以包括与查询匹配的任何类型的资源。
    - `"AWS::service-id::resource-type` – 以逗号分隔的资源类型规范字符串列表，其格式为：，例如 `"AWS::EC2::Instance"`。

  - `StackIdentifier`

    此元素指定要将其资源包含在组中的 AWS CloudFormation 堆栈的 Amazon 资源名称 (ARN)。

所有这些JSON元素都必须组合成JSON结构的单行字符串表示形式。例如，假设`Query`具有以下示例JSON结构的 a。此查询旨在仅匹配属于指定 AWS CloudFormation 堆栈的 Amazon S3 存储桶。

```
{
    "ResourceTypeFilters": [ "AWS::S3::Bucket" ],
    "StackIdentifier": "arn:aws:cloudformation:us-
west-2:123456789012:stack/MyCloudFormationStackName/fb0d5000-aba8-00e8-
aa9e-50d5cEXAMPLE"
}
```

它JSON可以表示为以下单行字符串，并用作`Query`元素的值。由于JSON结构的值必须是双引号字符串，因此必须对任何嵌入的双引号字符或正斜杠字符进行转义，方法是在每个字符前面加上反斜杠，如下所示：

```
"Query":"{\"ResourceTypeFilters\":[\"AWS::S3::Bucket\"],\"StackIdentifier\":
\"arn:aws:cloudformation:us-west-2:123456789012:stack\/MyCloudFormationStackName\/
fb0d5000-aba8-00e8-aa9e-50d5cEXAMPLE\"
```

然后将完整的`ResourceQuery`字符串表示为CLI命令参数，如下所示：

```
--resource-query '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"ResourceTypeFilters
\":[\"AWS::S3::Bucket\"],\"StackIdentifier\":\"arn:aws:cloudformation:us-
```

```
west-2:123456789012:stack\/MyCloudFormationStackName\/fb0d5000-aba8-00e8-
aa9e-50d5cEXAMPLE\"}'
```

构建基于标签的查询和创建组

以下过程说明了如何构建基于标签的查询和使用此查询创建资源组。

Console

1. 登录 AWS Resource Groups 控制台。
2. 在导航窗格中，选择创建资源组。
3. 在创建基于查询的组页面上的组类型下，选择基于标签组类型。
4. 在分组条件下，选择要包含在资源组中的资源类型。您最多可以在查询中包含 20 种资源类型。在本演练中，选择AWS::EC2::Instance AWS::S3::Bucket。
5. 仍在分组条件下，为标签指定标签键或标签键和值对，将匹配的资源限制为仅包含用指定值标记的资源。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。您可以通过在标签值之间添加 OR 运算符来为标签键添加多个值。要添加更多标签，请选择添加。查询将 AND 运算符分配给标签，以便与指定的资源类型和所有指定标签匹配的任何资源都将由查询返回。
6. 仍在 “分组条件” 下，选择 “预览组资源”，返回您账户中与指定标签密钥匹配的EC2实例和 S3 存储桶的列表。
7. 获得所需的结果后，根据此查询创建一个组。

   a. 在组详细信息下， 对于组名称，为您的资源组键入一个名称。

      资源组名称最多可以包含 128 个字符，包括字母、数字、连字符、句点和下划线。名称不能以 AWS 或 aws 开头。这些名称是预留的。资源组名称在您账户的当前区域中必须是唯一的。

   b. （可选）在组描述中，输入您的组的描述。

   c. （可选）在组标签中，添加仅适用于资源组（而不适用于组中的成员资源）的标签键和值对。

      如果计划将此组作为较大组的成员，则组标签非常有用。由于需要指定至少一个标签键以创建组，因此，请务必将组标签中的至少一个标签键添加到打算嵌套到更大组的组中。

8. 在完成后，选择创建组。

AWS CLI & AWS SDKs

基于标签的组基于 TAG_FILTERS_1_0 类型的查询。

1. 在 AWS CLI 会话中，键入以下内容，然后按 Enter，将群组名称、描述、资源类型、标签键和标签值的值替换为自己的值。描述最多可以包含 512 个字符，包括字母、数字、连字符、下划线、标点符号和空格。您最多可以在查询中包含 20 种资源类型。资源组名称最多可以包含 128 个字符，包括字母、数字、连字符、句点和下划线。名称不能以 AWS 或 aws 开头。这些名称是预留的。资源组名称在您的账户中必须是唯一的。

   需要使用至少一个 ResourceTypeFilters 值。要指定所有资源类型，请将 AWS::AllSupported 作为 ResourceTypeFilters 值。

```
$ aws resource-groups create-group \
    --name resource-group-name \
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"resource_type1\",\"resource_type2\"],\"TagFilters\":[{\"Key\":\"Key1\",
\"Values\":[\"Value1\",\"Value2\"]},{\"Key\":\"Key2\",\"Values\":[\"Value1\",
\"Value2\"]}]}"}'
```

   以下命令是一个示例。

```
$ aws resource-groups create-group \
    --name my-resource-group \
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"AWS::EC2::Instance\"],\"TagFilters\":[{\"Key\":\"Stage\",\"Values\":
[\"Test\"]}]}"}'
```

   以下命令是一个示例，其中包含所有支持的资源类型。

```
$ aws resource-groups create-group \
    --name my-resource-group \
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"AWS::AllSupported\"],\"TagFilters\":[{\"Key\":\"Stage\",\"Values\":[\"Test
\"]}]}"}'
```

2. 在对命令的响应中返回以下内容。

   - 您创建的组的完整描述。
   - 您用于创建组的资源查询。

- 与组关联的标签。

创建基于 AWS CloudFormation 堆栈的群组

以下过程说明了如何构建基于堆栈的查询和使用此查询创建资源组。

Console

1. 登录 AWS Resource Groups 控制台。
2. 在导航窗格中，选择创建资源组。
3. 在创建基于查询的群组中，在群组类型下，选择基于CloudFormation 堆栈的群组类型。
4. 选择要作为组基础的堆栈。只能将资源组基于一个堆栈。要筛选堆栈列表，请开始键入堆栈的名称。仅在列表中显示具有支持的状态的堆栈。
5. 在堆栈中选择要包含在组中的资源类型。对于本演练，请保留默认值所有受支持的资源类型。有关可以包含在组中的受支持资源类型的更多信息，请参阅可以与标签编辑器一起 AWS Resource Groups 使用的资源类型。
6. 选择查看组资源以返回 AWS CloudFormation 堆栈中与所选资源类型相匹配的资源列表。
7. 获得所需的结果后，根据此查询创建一个组。

   a. 在组详细信息下， 对于组名称，为您的资源组键入一个名称。

      资源组名称最多可以包含 128 个字符，包括字母、数字、连字符、句点和下划线。名称不能以 AWS 或 aws 开头。这些名称是预留的。资源组名称在您账户的当前区域中必须是唯一的。

   b. （可选）在组描述中，输入您的组的描述。

   c. （可选）在组标签中，添加仅适用于资源组（而不适用于组中的成员资源）的标签键和值对。

      如果计划将此组作为较大组的成员，则组标签非常有用。由于需要指定至少一个标签键以创建组，因此，请务必将组标签中的至少一个标签键添加到打算嵌套到更大组的组中。

8. 在完成后，选择创建组。

AWS CLI & AWS SDKs

AWS CloudFormation 基于堆栈的组基于类型的查询。`CLOUDFORMATION_STACK_1_0`

1. 运行以下命令，将组名称、描述、堆栈标识符和资源类型的值替换为您自己的值。描述最多可以包含 512 个字符，包括字母、数字、连字符、下划线、标点符号和空格。

   如果未指定资源类型，则 Resource Groups 包含堆栈中的所有支持的资源类型。您最多可以在查询中包含 20 种资源类型。资源组名称最多可以包含 128 个字符，包括字母、数字、连字符、句点和下划线。名称不能以 AWS 或 aws 开头。这些名称是预留的。资源组名称在您的账户中必须是唯一的。

   这些区域有：*stack_identifier* 是堆栈ARN，如示例命令所示。

   ```
   $ aws resource-groups create-group \
       --name group_name \
       --description "description" \
       --resource-query
    '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
   \"stack_identifier\",\"ResourceTypeFilters\":[\"resource_type1\",
   \"resource_type2\"]}"}'
   ```

   以下命令是一个示例。

   ```
   $ aws resource-groups create-group \
       --name My-CFN-stack-group \
       --description "My first CloudFormation stack-based group" \
       --resource-query
    '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
   \"arn:aws:cloudformation:us-west-2:123456789012:stack\/AWStestuseraccount\/
   fb0d5000-aba8-00e8-aa9e-50d5cEXAMPLE\",\"ResourceTypeFilters\":
   [\"AWS::EC2::Instance\",\"AWS::S3::Bucket\"]}"}'
   ```

2. 在对命令的响应中返回以下内容。

   - 您创建的组的完整描述。
   - 您用于创建组的资源查询。

更新中的群组 AWS Resource Groups

要在 Resource Groups 中更新基于标签的资源组，您可以编辑作为组基础的查询和标签。只能通过对查询或标签应用更改来在组中添加和删除资源。不能选择要在组中添加或删除的特定资源。在组中添加或移除特定资源的最佳方法是编辑该资源的标签。然后，验证您的资源组标签查询是包含还是省略该标签，具体取决于您是否希望资源加入您的组。

要更新 AWS CloudFormation 基于堆栈的资源组，可以选择其他堆栈。您还可以在堆栈中添加或移除要加入该组的资源类型。要更改堆栈中可用的资源，请更新用于创建堆栈的 AWS CloudFormation 模板，然后在中更新堆栈 AWS CloudFormation。有关如何更新 AWS CloudFormation 堆栈的更多信息，请参阅《AWS CloudFormation 用户指南》中的AWS CloudFormation 堆栈更新。

在中 AWS CLI，您可以用两个命令更新群组。

- `update-group`，用于更新组的描述。
- `update-group-query`，用于更新用于确定组成员资源的资源查询和标签。

在控制台中，您无法将基于 AWS CloudFormation 堆栈的组更改为基于标签的查询组，反之亦然。但是，您可以使用资源组（Resource Groups）来做到这一点API，包括在 AWS CLI。

更新基于标签的查询组

以下过程向您展示如何更新基于标签的查询组。

Console

可以在查询中更改组所基于的资源类型或标签以更新基于标签的组。您还可以添加或更改组的描述。

1. 登录 AWS Resource Groups 控制台。
2. 在导航窗格中的保存的资源组下面，选择该组的名称，然后选择编辑。

> **Note**
>
> 您只能更新自己拥有的资源组。所有者列显示每个资源组的账户所有权。账户所有者不是您已登录账户的任何组都是在 AWS License Manager中创建的。有关更多信息，请参阅 License Manager 用户指南中的 AWS License Manager中的主机资源组。

3. 在编辑组页面上的分组条件下，添加或移除资源类型。您最多可以在查询中包含 20 种资源类型。要删除资源类型，请在该资源类型的标签上选择 X。选择查看组资源以查看更改如何影响您的组的资源成员。在本演练中，我们将资源类型AWS::RDS: DBInstance 添加到查询中。
4. 仍在分组条件下，根据需要编辑标签。在该示例中，我们筛选具有 Stage 标签键并添加 Test 标签值的资源。标签值是可选的，但会进一步缩小查询的结果。要删除标签，请在其标签上选择 X。
5. 在其他信息中，您可以编辑组描述。在创建组后，您无法编辑组的名称。
6. （可选）在组标签中，您可以添加或移除标签。组标签是有关资源组的元数据。它们不会影响成员资源。要更改资源组的查询返回的资源，请在分组条件下编辑标签。

   如果计划将此组作为较大组的成员，则组标签非常有用。要创建组，必须至少指定标签键。因此，请务必在组标签中为计划嵌套到较大组中的组添加至少一个标签键。
7. 选择预览组资源以检索您的账户中与指定标签密钥匹配的EC2实例、S3 存储桶和 Amazon RDS 数据库实例的更新列表。如果在列表中看不到所需的资源，请确保使用在分组条件中指定的标签标记了资源。
8. 在完成后，选择保存更改。

AWS CLI & AWS SDKs

在中 AWS CLI，您可以使用两个不同的命令更新群组的查询并更新资源组的描述。不能编辑现有组的名称。在中 AWS CLI，您可以将基于标签的组更改为基于 CloudFormation 堆栈的组，反之亦然。

1. 如果您不想更改组的描述，请跳过此步骤并转到下一步。在 AWS CLI 会话中，键入以下内容，然后按 Enter，将群组名称和描述的值替换为自己的值。

```
$ aws resource-groups update-group \
    --group-name resource-group-name \
    --description "description_text"
```

以下命令是一个示例。

```
$ aws resource-groups update-group \
    --group-name my-resource-group \
    --description "EC2 instances, S3 buckets, and RDS DBs that we are using for
 the test stage."
```

该命令会返回一个完整、更新的组描述。

2. 要更新组的查询和标签，请键入以下命令。将组名称、资源类型、标签键和标签值替换为您自己的值。然后按 Enter。您最多可以在查询中包含 20 种资源类型。

```
$ aws resource-groups update-group-query \
    --group-name resource-group-name \
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"resource_type1\",\"resource_type2\"],\"TagFilters\":[{\"Key\":\"Key1\",
\"Values\":[\"Value1\",\"Value2\"]},{\"Key\":\"Key2\",\"Values\":[\"Value1\",
\"Value2\"]}]}"}'
```

以下命令是一个示例。

```
$ aws resource-groups update-group-query \
    --group-name my-resource-group \
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"AWS::EC2::Instance\",\"AWS::S3::Bucket\",\"AWS::RDS::DBInstance\"],
\"TagFilters\":[{\"Key\":\"Stage\",\"Values\":[\"Test\"]}]}"}'
```

该命令会返回已更新的查询作为结果。

更新基于 AWS CloudFormation 堆栈的群组

以下过程向您展示如何更新 CloudFormation 基于堆栈的组。

Console

您无法在中将 AWS CloudFormation 基于堆栈的组更改为基于标签的组。 AWS Management Console但是，您可以更改该组所基于的堆栈，也可以更改要包含在组中的堆栈资源类型。您还可以添加或更改组的描述。

1. 登录 AWS Resource Groups 控制台。
2. 在导航窗格中的保存的资源组下面，选择该组的名称，然后选择编辑。

3.
> **Note**
>
> 您只能更新自己拥有的资源组。所有者列显示每个资源组的账户所有权。账户所有者不是您已登录账户的任何组都是在 AWS License Manager中创建的。有关更多信息，请参阅 License Manager 用户指南中的 AWS License Manager中的主机资源组。

4. 在编辑组页面上的分组条件下，要更改组所基于的堆栈，请从下拉列表中选择该堆栈。只能将资源组基于一个堆栈。要筛选堆栈列表，请开始键入堆栈的名称。仅在列表中显示具有支持的状态的堆栈。有关支持的状态列表，请参阅本指南中的在中创建基于查询的群组 AWS Resource Groups。
5. 添加或删除资源类型。仅在下拉列表中显示堆栈中的可用资源类型。默认值为所有受支持的资源类型。您最多可以在查询中包含 20 种资源类型。要删除资源类型，请在该资源类型的标签上选择 X。有关可以包含在组中的受支持资源类型的更多信息，请参阅可以与标签编辑器一起 AWS Resource Groups 使用的资源类型。
6. 选择预览组资源以检索 AWS CloudFormation 堆栈中与所选资源类型相匹配的资源列表。
7. 在其他信息中，您可以编辑组描述。在创建组后，您无法编辑组的名称。
8. 在组标签中，添加或删除标签。组标签是有关资源组的元数据。它们不会影响成员资源。要更改资源组的查询返回的资源，请在分组条件中编辑标签。

   如果计划将此组作为较大组的成员，则组标签非常有用。要创建组，必须至少指定标签键。因此，请务必在组标签中为计划嵌套到较大组中的组添加至少一个标签键。
9. 在完成后，选择保存更改。

AWS CLI & AWS SDKs

在中 AWS CLI，您可以使用两个不同的命令更新群组的查询并更新资源组的描述。不能编辑现有组的名称。在中 AWS CLI，您可以将基于标签的组更改为基于 CloudFormation 堆栈的组，反之亦然。

1. 如果您不想更改组的描述，请跳过此步骤并转到下一步。运行以下命令，将组名称和描述的值替换为自己的值。

```
$ aws resource-groups update-group \
    --group-name "resource-group-name" \
    --description "description_text"
```

   以下命令是一个示例。

```
$ aws resource-groups update-group \
    --group-name "My-CFN-stack-group" \
    --description "EC2 instances, S3 buckets, and RDS DBs that we are using for
 the test stage."
```

该命令会返回一个完整、更新的组描述。

2. 要更新组的查询和标签，请运行以下命令。将组名称、堆栈标识符和资源类型的值替换为您自己的值。要添加资源类型，请在命令中提供完整的资源类型列表，而不是仅提供添加的资源类型。您最多可以在查询中包含 20 种资源类型。

   这些区域有：*stack_identifier* 是堆栈ARN，如示例命令所示。

```
$ aws resource-groups update-group-query \
    --group-name resource-group-name \
    --description "description" \
    --resource-query
 '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
\"stack_identifier\",\"ResourceTypeFilters\":[\"resource_type1\",
\"resource_type2\"]}"}'
```

以下命令是一个示例。

```
$ aws resource-groups update-group-query \
    --group-name "my-resource-group" \
    --description "Updated CloudFormation stack-based group" \
    --resource-query
 '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
\"arn:aws:cloudformation:us-west-2:810000000000:stack\/AWStestuseraccount
\/fb0d5000-aba8-00e8-aa9e-50d5cEXAMPLE\",\"ResourceTypeFilters\":
[\"AWS::EC2::Instance\",\"AWS::S3::Bucket\"]}"}'
```

该命令会返回已更新的查询作为结果。

组生命周期事件：监控资源组的更改

使用 AWS Resource Groups 将资源组织成组后，您可以监视这些组中是否有作为事件向您公开的更改。您可以收到有关组活动的通知，以此作为您采取某种操作的信号。例如，您可以配置在组成员资格发生更改时发送的通知。您可以使用添加新组成员时发生的事件来触发 Lambda 函数，该函数以编程方式审查更改，以确保新的组成员符合组织设定的合规性要求。此类 Lambda 函数可以对任何未能满足这些要求的新组成员执行自动补救措施。因移除组成员而导致的事件可能会触发 Lambda 函数，该函数执行任何必要的清理，例如删除链接的资源。

通过为资源组开启群组生命周期事件，您可以允许 Amazon 捕获有关群组变更的事件， EventBridge 并将其提供给所有受 EventBridge 支持的目标服务。然后，您可以将这些目标服务配置为自动执行场景所需的任何操作。这些目标包括各种 AWS 服务，例如亚马逊简单通知服务 (亚马逊SNS)、亚马逊简单队列服务 (亚马逊SQS) 和 AWS Lambda。借助 Lambda 之类的服务，您的事件可以触发使用代码执行所需操作的编程响应。有关您可以定位的 AWS 服务列表 EventBridge，请参阅《亚马逊 EventBridge 用户指南》中的亚马逊 EventBridge 目标。

开启群组生命周期事件时， AWS Resource Groups 会创建以下项目：

- 一个 AWS Identity and Access Management (IAM) 服务相关角色，有权监控您的资源标签是否有任何更改，并有权监控 AWS CloudFormation 堆栈中资源的任何更改。
- Resource Groups 托管 EventBridge 规则，用于捕获资源的任何标签或堆栈更改的详细信息。EventBridge 使用此规则将这些更改通知资源组。然后，Resource Groups 会生成要发送的成员资格事件， EventBridge 供您的自定义规则处理。

服务关联角色只能由 Resource Groups 服务担任。有关 Resource Groups 为此功能使用的服务关联角色的更多信息，请参阅 为 Resource Groups 使用服务相关角色。

开启此功能后，当您对资源组进行以下任何更改时，Resource Groups 会生成一个事件：

- 创建新资源组。
- 更新定义基于查询的资源组成员资格的查询。
- 更新服务关联资源组的配置。
- 更新资源组的描述。
- 删除资源组。
- 通过在资源组中添加或移除资源来更改资源组的成员资格。当标签更改或 AWS CloudFormation 堆栈发生变化时，也可能发生成员资格变更。

Important

- 要成功接收和响应群组事件，必须同时对 Resource Groups 和 EventBridge。您可以按任意顺序执行更改，但是在您对两个服务进行更改之前，不会将任何群组事件发布到 EventBridge 目标。
- 资源组的更改不包括对附加到资源组本身的任何标签的更改。要根据群组的标签更改生成事件，必须使用使用`aws.tag`源而不是来源的 EventBridge `aws.resource-groups`规则。有关更多信息，请参阅 Amazon EventBridge 用户指南中的AWS 资源标签变更事件。

主题

在 Resource Groups 中开启组生命周期事件

要接收有关资源组生命周期更改的通知，可以在组生命周期事件上接收通知。然后，Resource Groups 会提供有关您的群组对亚马逊 EventBridge的更改的信息。在中 EventBridge，您可以使用您在 EventBridge 服务中定义的规则来评估变更并采取行动。

最小权限

要在中开启群组生命周期事件 AWS 账户，您必须以具有以下权限的 AWS Identity and Access Management (IAM) 委托人身份登录：

- `resource-groups:UpdateAccountSettings`
- `iam:CreateServiceLinkedRole`
- `events:PutRule`
- `events:PutTargets`
- `events:DescribeRule`
- `events:ListTargetsByRule`

- cloudformation:DescribeStacks
- cloudformation:ListStackResources
- tag:GetResources

当您最初在中打开群组生命周期事件时 AWS 账户，Resource Groups 会创建一个名为AWSServiceRoleForResourceGroups的服务相关角色。此托管角色有权使用 Resource Groups 托管 EventBridge 规则。该规则会监控附加到您资源的标签以及您账户中的 AWS CloudFormation 堆栈是否有任何更改。然后，Resource Groups 将这些更改发布到亚马逊的默认事件总线 EventBridge。该服务还会创建名为的 EventBridge 托管规则Managed.ResourceGroups.TagChangeEvents。此规则捕获您的资源标签更改的详细信息。这样，Resource Groups 就可以生成要发送的成员资格事件， EventBridge 供您的自定义规则处理。然后，您的 EventBridge 规则可以通过向规则的配置目标发送通知来响应事件。

完成这些步骤后，查找这些事件的规则应该会在几分钟后开始接收它们。

你可以使用或使用来自 AWS Management Console 或其中一个 SDK API 的命令来开启群组生命周期事件。 AWS CLI

> **Note**
>
> 如果您的资源组配额过高，则无法开启组生命周期事件。有关更多信息，请查看查看服务配额。

AWS Management Console

在 Resource Groups 控制台中开启组生命周期事件

1. 在 Resource Groups 控制台中打开设置页面。
2. 在组生命周期事件部分中，选择通知已关闭旁边的开关。
3. 在确认对话框中，选择开启通知。

   功能开关显示通知已开启。

至此，该过程的第一部分完成。开启事件通知后，您可以在 Amazon 中创建规则 EventBridge，捕获事件并将其发送给特定机构 AWS 服务 进行处理。

AWS CLI

使用 AWS CLI 或 AWS SDK 开启群组生命周期事件

以下示例演示如何使用在 Resourc AWS CLI e Groups 中开启群组生命周期事件。输入带有服务主体参数的命令，如图所示。输出显示该功能的当前状态和所需状态。

```
$ aws resource-groups update-account-settings \
    --group-lifecycle-events-desired-status ACTIVE
{
    "AccountSettings": {
        "GroupLifecycleEventsDesiredStatus": "ACTIVE",
        "GroupLifecycleEventsStatus": "IN_PROGRESS"
    }
}
```

您可以通过运行以下示例命令来确认该功能已开启。当两个状态字段显示相同的值时，操作即告完成。

```
$ aws resource-groups get-account-settings
{
    "AccountSettings": {
        "GroupLifecycleEventsDesiredStatus": "ACTIVE",
        "GroupLifecycleEventsStatus": "ACTIVE"
    }
}
```

有关更多信息，请参阅以下资源：

- AWS CLI — aw s 资源组 update-account-settings和 aws 资源组 get-account-settings
- API — UpdateAccountSettings以及 GetAccountSettings

创建用于捕获群组生命周期事件和发布通知的 EventBridge 规则

您可以在中为资源组开启群组生命周期事件，将事件发布AWS Resource Groups到 Amazon EventBridge。然后，您可以通过将这些事件发送给其他人进行进一步处理来创建响应这些事件AWS 服务的 EventBridge规则。

AWS CLI

在中创建用于捕 EventBridge 获事件并将其发送到所需目标服务的规则的过程需要两个单独的 CLI 命令：

1. 创建 EventBridge 规则以捕获您想要的事件
2. 将可以处理事件的目标附加到 EventBridge 规则

步骤 1：创建捕获事件的 EventBridge 规则

以下AWS CLI`put-rule`示例命令创建了一 EventBridge 条规则，用于捕获所有 Resource Groups 生命周期事件更改。

```
$ aws events put-rule \
    --name "CatchAllResourceGroupEvents" \
    --event-pattern '{"source":["aws.resource-groups"]}'
{
    "RuleArn": "arn:aws:events:us-east-1:123456789012:rule/
CatchAllResourceGroupEvents"
}
```

输出包含新规则的 Amazon 资源名称（ARN）。

> **Note**
>
> 根据您使用的操作系统和 Shell，包含引用字符串的参数值具有不同的格式规则。对于本指南中的示例，我们展示了在 Linux BASH Shell 上运行的命令。有关为其他操作系统（例如 Windows 命令提示符）格式化带有嵌入式引号的字符串的说明，请参阅 AWS Command Line Interface 用户指南中的在字符串中使用引号。
> 随着参数字符串变得越来越复杂，接受文本文件中的参数值而不是直接在命令行中键入参数值会更容易，也更不容易出错。

以下事件模式将事件限制为仅与指定组相关的、由其 ARN 标识的事件。此事件模式是一个复杂的 JSON 字符串，当压缩成单行、正确转义的 JSON 字符串时，其可读性要低得多。您可以改为将其存储在文件中。

将事件模式 JSON 字符串存储在文件中。在下面的代码示例中，文件为`eventpattern.txt`。

```
{
    "source": [ "aws.resource-groups" ],
    "detail": {
        "group": {
            "arn": [ "my-resource-group-arn" ]
        }
    }
}
```

然后，发出以下命令来创建规则，并且从文件中检索自定义事件模式。

```
$ aws events put-rule \
    --name "CatchResourceGroupEventsForMyGroup" \
    --event-pattern file://eventpattern.txt
{
    "RuleArn": "arn:aws:events:us-east-1:123456789012:rule/
CatchResourceGroupEventsForMyGroup"
}
```

要捕获其他类型的 Resource Groups 事件，请将 `--event-pattern` 字符串替换为 不同用例的 EventBridge 自定义事件模式示例 部分中显示的筛选条件。

步骤 2：将可以处理事件的目标附加到 EventBridge 规则

现在，您已经具有捕获感兴趣事件的规则，可以附加一个或多个目标来对事件进行某种类型的处理。

以下 AWS CLI `put-targets` 命令将名为 `my-sns-topic` 的 Amazon Simple Notification Service（Amazon SNS）主题附加到前述示例中创建的规则。当规则中指定的组发生更改时，该主题的所有订阅者都会收到通知。

```
$ aws events put-targets \
    --rule CatchResourceGroupEventsForMyGroup \
    --targets Id=1,Arn=arn:aws:sns:us-east-1:123456789012:my-sns-topic
{
    "FailedEntryCount": 0,
    "FailedEntries": []
}
```

此时，任何与规则中的事件模式相匹配的组更改都将自动发送到已配置的一个或多个目标。如上例所示，如果目标是 Amazon SNS 主题，则该主题的所有订阅者都会收到一条包含该事件的消息，如 Resource Groups 生命周期事件的结构和语法 中所述。

有关更多信息，请参阅以下资源：

- AWS CLI – aws events put-rule 和 aws events put-targets
- API — PutRule以及 PutTargets

创建仅捕获特定组生命周期事件类型的规则

您可以使用自定义事件模式创建规则，该模式仅捕获您感兴趣的事件。有关如何使用自定义事件模式筛选传入事件的完整详情，请参阅《亚马逊 EventBridge 用户指南》中的 Amazon EventBridge 事件。

例如，假设您希望规则仅处理指示创建新资源组的 Resource Groups 通知。您可以使用类似于以下示例的自定义事件模式。

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group State Change" ],
    "detail": {
        "state-change": "create"
    }
}
```

该筛选条件仅捕获在指定字段中具有精确值的事件。有关可供您匹配的字段的完整列表，请参阅 Resource Groups 生命周期事件的结构和语法。

关闭组生命周期事件

您可以关闭组生命周期事件以阻止 AWS Resource Groups 向 Amazon EventBridge 发出事件。可通过以下两种方式完成此操作：使用 AWS Management Console 或者通过使用 AWS CLI 或其中一个 SDK API。

> **Note**
>
> 关闭组生命周期事件会删除 Resource Groups 托管 EventBridge 规则，该规则用于扫描资源标签和 AWS CloudFormation 堆栈是否有更改。Resource Groups 无法再将这些更改传递给 EventBridge。您在 EventBridge 中定义的任何查找 Resource Groups 事件的规则都会停止接收要处理的事件。如果您打算将来再次开启组生命周期事件，则可以禁用您的规则。如果您不打算再次使用这些规则，则可以删除它们。有关更多信息，请参阅 Amazon EventBridge 用户指南中的禁用或删除 EventBridge 规则

关闭组生命周期事件不会删除服务关联角色。如果您希望使用 IAM，则可以手动删除服务关联角色。如果您稍后需要再次开启组生命周期事件，而服务关联角色不存在，Resource Groups 会自动重新创建该角色。

最小权限

要在当前 AWS 账户 中关闭组生命周期事件，您必须以具有以下权限的 AWS Identity and Access Management（IAM）主体身份登录：

- `resource-groups:UpdateAccountSettings`
- `events:DeleteRule`
- `events:RemoveTargets`
- `events:DescribeRule`
- `events:ListTargetsByRule`

AWS Management Console

关闭向 EventBridge 发送的组生命周期事件通知

1. 在 Resource Groups 控制台中打开设置页面。
2. 在组生命周期事件部分中，选择通知已开启旁边的开关。
3. 在确认对话框中，选择关闭通知。

   将显示功能开关：事件通知已关闭。

此时，Resource Groups 不再向 EventBridge 的默认事件总线发送事件，并且您拥有的任何规则都不再接收要处理的组通知事件。您可以选择删除这些规则以完成清理。

AWS CLI

关闭向 EventBridge 发送的组生命周期事件通知

以下示例说明如何使用 AWS CLI 来关闭 Resource Groups 中的组生命周期事件。

```
$ aws resource-groups update-account-settings \
    ----group-lifecycle-events-desired-status INACTIVE
{
```

```
    "AccountSettings": {
        "GroupLifecycleEventsDesiredStatus": "INACTIVE",
        "GroupLifecycleEventsStatus": "INACTIVE"
    }
}
```

有关更多信息，请参阅以下资源：

- AWS CLI – aws resource-groups update-account-settings 和 aws resource-groups get-account-settings
- API – UpdateAccountSettings 和 GetAccountSettings

Resource Groups 生命周期事件的结构和语法

主题

- detail 字段的结构
- 不同用例的 EventBridge 自定义事件模式示例

的生命周期事件 AWS Resource Groups 采用JSON对象字符串的形式，一般格式如下。

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group ... Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/MyGroupName"
    ],
    "detail": {
        ...
    }
}
```

有关所有亚马逊 EventBridge 事件的通用字段的详细信息，请参阅《亚马逊 EventBridge 用户指南》中的亚马逊 EventBridge 事件。下表说明了特定于 Resource Groups 的详细信息。

字段名称	类型	描述
detail-type	String	对于 Resource Groups，detail-type 字段始终是以下值之一： • ResourceGroups Group State Change – 表示整体组状态及其属性的更改。 • ResourceGroups Group Membership Change – 表示群组成员资格的更改。
source	String	对于 Resource Groups，此值始终为 "aws.resource-groups" 。
resources	一组 Amazon 资源名称 (ARNs)	此字段始终包含触发此事件的群组的 Amazon 资源名称 (ARN)。 如果适用，此字段还可以包括添加到该ARNs组或从该组中移除的所有资源。
detail	JSON对象字符串	这是事件的有效负载。detail 字段的内容根据 detail-type 的值而变化。有关更多信息，请参见下一节。

detail 字段的结构

detail 字段包含有关特定更改的所有 Resource Groups 服务特定详细信息。根据上一节中描述的 detail 字段值，该 detail-type 字段可以采用两种形式之一，即组状态更改或成员资格更改。

> **Important**
>
> 这些事件中的资源组由组ARN和包含的"unique-id"字段的组合来标识UUID。通过将UUID作为资源组标识的一部分，可以区分已删除的组和以后使用相同名称创建的另一个组。我们建议您将ARN和唯一 ID 的串联视为程序中与这些事件交互的群组的密钥。

组状态更改

```
"detail-type": "ResourceGroups Group State Change"
```

此 detail-type 值表示组本身的状态（包括其元数据）已更改。此更改发生在创建、更新或删除组时，如 detail 中的 "change" 字段所示。

指定此 detail-type 时，details 部分中包含的信息包括下表中描述的字段。

字段名称	类型	描述
event-sequence	Double	一个单调递增的数字，用于指定特定组的事件顺序。当您删除该组并创建另一个同名的组时，该数字会重置。
group	GroupJSON对象	按事件ARN、名称和唯一 ID 与事件关联的群组对象。
state-change	String	发生的状态更改类型。可以是以下任何值： • create • update • delete
old-state	GroupState JSON对象	更改前的组状态。该对象仅包含已更改的属性的值。
new-state	GroupState JSON对象	更改后的组状态。该对象仅包含已更改的属性的值。

该groupJSON对象包含下表中描述的元素。

字段名称	类型	描述
arn	String	该ARN组的。
name	String	组的友好名称。
unique-id	GUID	一个唯一GUID值，用于区分已删除的群组和后来使用相同名称和ARN创建的另一个群组。在代码中使用这些事件时，请使用ARN和此值的串联作为该组的唯一键。

这些GroupStateJSON对象包含下表中描述的元素。

字段名称	类型	描述
description	String	资源组的客户提供描述。
resource-query	ResourceQuery JSON对象	定义群组成员的查询的JSON表示形式。此字段仅适用于基于查询的组。此字段的语法由ResourceQuery API数据类型定义。创建和更新事件示例中包含了这方面的示例。
group-configuration	Configuration JSON对象	与服务关联组关联的配置参数的JSON表示形式。有关更多信息，请参阅《AWS Resource Groups API参考资料》中的资源组服务配置。

以下每个代码示例说明了每种 state-change 类型的 detail 字段内容。

创建

"state-change": "create"

该事件表示新组已创建。该事件包含组创建期间设置的所有组元数据属性。除非组为空，否则此事件之后通常会有一个或多个组成员资格事件。具有空值的属性不会显示在事件正文中。

以下示例事件表示名为 my-service-group 的新建资源组。在此示例中，该组使用基于标签的查询，该查询仅匹配具有该标签"project"="my-service"的亚马逊弹性计算云 (AmazonEC2) 实例。

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group State Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-group"
    ],
    "detail": {
        "event-sequence": 1.0,
```

```
        "state-change": "create",
        "group": {
            "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-
group",
            "name": "my-service-group",
            "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceea"
        },
        "new-state": {
            "resource-query": {
                "type": "TAG_FILTERS_1_0",
                "query": "{
                    \"ResourceTypeFilters\": [\"AWS::EC2::Instance\"],
                    \"TagFilters\": [{\"Key\":\"project\", \"Values\":[\"my-service\"}]
                }"
            }
        }
    }
}
```

更新

`"state-change": "update"`

该事件表示现有组已按某种方式修改。该事件仅包含从先前状态更改的属性。未更改的属性不会显示在事件正文中。

以下示例事件表明，上一个示例的资源组中基于标签的查询已被修改为在该组中也包含 Amazon EC2 卷资源。

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group State Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-group"
    ],
    "detail": {
        "event-sequence": 3.0,
        "state-change": "update",
```

```
        "group": {
            "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-
group",
            "name": "my-service",
            "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceea"
        },
        "new-state": {
            "resource-query": {
                "type": "TAG_FILTERS_1_0",
                "query": "{
                    \"ResourceTypeFilters\": [\"AWS::EC2::Instance\",
 \"AWS::EC2::Volume\"],
                    \"TagFilters\": [{\"Key\":\"project\", \"Values\":[\"my-service\"}]
                }"
            }
        },
        "old-state": {
            "resource-query": {
                "type": "TAG_FILTERS_1_0",
                "query": "{
                    \"ResourceTypeFilters\": [\"AWS::EC2::Instance\"],
                    \"TagFilters\": [{\"Key\":\"Project\", \"Values\":[\"my-service\"}]
                }"
            }
        }
    }
}
```

删除

`"state-change": "delete"`

该事件表示现有组已被删除。除了组标识外，详细信息字段不包含关于组的元数据。该 `event-sequence` 字段将在此事件之后重置，因为根据定义，它是此 `arn` 和 `unique-id` 的最后一个事件。

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group State Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
```

```
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/my-service"
    ],
    "detail": {
        "event-sequence": 4.0,
        "state-change": "delete",
        "group": {
            "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service",
            "name": "my-service",
            "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceea"
        }
    }
}
```

组成员资格更改

`"detail-type": "ResourceGroups Group Membership Change"`

此 `detail-type` 值表示该组的成员资格因向该组添加资源或从组中移除资源而更改。指定`detail-type`此字段后，顶级`resources`字段将ARN包括成员资格已更改ARNs的群组以及向该组中添加或移除的所有资源。

指定此 `detail-type` 时，`details` 部分中包含的信息包括下表中描述的字段。

字段名称	类型	描述
`event-sequence`	Double	一个单调递增的数字，表示特定组的事件顺序。当组被删除且其唯一 ID 更改时，该数字会重置。
`group`	`Group`JSON对象	通过事件的群组对象ARN、名称和唯一 ID 来标识与事件关联的群组对象。
`resources`	`ResourceChange` JSON对象数组	组成员资格已更改的资源数组。 此 `ResourceChange` 对象包含每个资源的以下字段： • `membership-change` – 该值为 `"add"` 或 `"remove"`。 • `arn`— 已添加或移除ARN的资源的。

字段名称	类型	描述
		• resource-type – 添加或移除的资源类型。

以下代码示例说明了典型成员资格更改类型的事件内容。此示例显示正在向组中添加一个资源，以及从该组中移除一个资源。

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group Membership Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/my-service",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-efef2222"
    ],
    "detail": {
        "event-sequence": 2.0,
        "group": {
            "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service",
            "name": "my-service",
            "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceea"
        },
        "resources": [
            {
                "membership-change": "add",
                "arn": "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111",
                "resource-type": "AWS::EC2::Instance"
            },
            {
                "membership-change": "remove",
                "arn": "arn:aws:ec2:us-east-1:123456789012:instance/i-efef2222",
                "resource-type": "AWS::EC2::Instance"
            }
        ]
    }
}
```

不同用例的 EventBridge 自定义事件模式示例

以下示例 EventBridge 自定义事件模式会筛选由 Resource Groups 生成的事件，仅显示您对特定事件规则和目标感兴趣的事件。

在以下代码示例中，如果需要特定的组或资源，请替换每个 *user input placeholder* 用你自己的信息。

所有 Resource Groups 事件

```
{
    "source": [ "aws.resource-groups" ]
}
```

组状态或成员资格更改事件

以下代码示例适用于所有组状态更改。

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group State Change " ]
}
```

以下代码示例适用于所有组成员资格更改。

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change" ]
}
```

特定组的事件

```
{
    "source": [ "aws.resource-groups" ],
    "detail": {
        "group": {
            "arn": [ "my-group-arn" ]
        }
    }
}
```

前面的示例捕获了对指定组的更改。以下示例执行相同的操作，并且还会捕获该组是另一个组的成员资源时的更改。

```
{
    "source": [ "aws.resource-groups" ],
    "resources": [ "my-group-arn" ]
}
```

特定资源的事件

您只能筛选特定成员资源的组成员资格更改事件。

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change " ],
    "resources": [ "arn:aws:ec2:us-east-1:123456789012:instance/i-b188560f" ]
}
```

特定资源类型的事件

您可以使用前缀匹配ARNs来匹配特定资源类型的事件。

```
{
    "source": [ "aws.resource-groups" ],
    "resources": [
        { "prefix": "arn:aws:ec2:us-east-1:123456789012:instance" }
    ]
}
```

或者，您可以通过使用 `resource-type` 标识符来使用精确匹配，从而可以简洁地匹配多个类型。与前面的示例不同，以下示例仅匹配组成员资格更改事件，因为组状态更改事件的 `detail` 字段中不包含字段 `resources`。

```
{
    "source": [ "aws.resource-groups" ],
    "detail": {
        "resources": {
                "resource-type": [ "AWS::EC2::Instance", "AWS::EC2::Volume" ]
         }
    }
}
```

所有资源移除事件

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change" ],
    "detail": {
        "resources": {
                "membership-change": [ "remove" ]
        }
    }
}
```

特定资源的所有资源移除事件

```
 {
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change" ],
    "detail": {
        "resources": {
                "membership-change": [ "remove" ],
                "arn": [ "arn:aws:ec2:us-east-1:123456789012:instance/i-b188560f" ]
         }
    }
}
```

您不能使用本节第一个示例中使用的顶级 `resources` 数组进行此类事件筛选。这是因为顶级 `resources` 元素中的资源可能是添加到组中的资源，并且该事件仍然会匹配。换句话说，以下代码示例可能会返回意外事件。相反，请使用上一个示例中显示的语法。

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change" ],
    "resources": [ "arn:aws:ec2:us-east-1:123456789012:instance/i-b188560f" ],
    "detail": {
        "resources": {
                "membership-change": [ "remove" ]
         }
     }
}
```

从中删除资源组 AWS Resource Groups

您可以使用AWS Resource Groups 控制台或从 AWS CLI 中删除资源组 AWS Resource Groups。删除资源组不会删除作为组成员的资源或成员资源上的标签。它仅删除组结构和任何组级别标签。

Console

要删除资源组

1. 登录 AWS Resource Groups 控制台。
2. 在导航窗格中，选择保存的资源组。
3. 请选择要删除的资源组的名称，然后选择查看详细信息。
4. 在组的详细信息页面上，请选择右上角的删除。
5. 在提示您确认删除时，选择删除。

AWS CLI & AWS SDKs

要删除资源组

1. 运行以下命令，替换 *resource_group_name* 用你的群组的名字。

```
$ aws resource-groups delete-group \
    --group-name resource_group_name
```

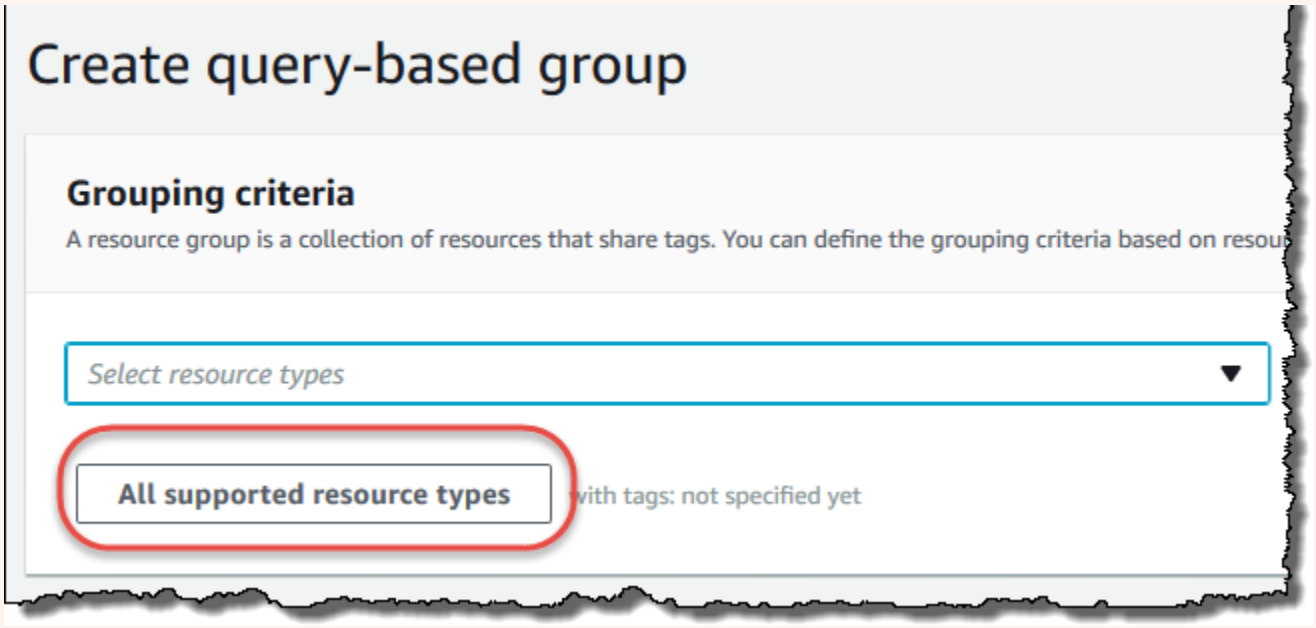
2. 在提示您确认删除时，键入 yes，然后按 Enter。

可以与标签编辑器一起 AWS Resource Groups 使用的资源类型

您可以使用 AWS Management Console 或创建资源组 AWS CLI ，然后通过这些组与成员资源进行交互。您可以为许多 AWS 资源添加标签，然后使用这些标签来管理群组成员资格。本主题介绍您可以使用将哪些 AWS 资源类型包含在资源组中 AWS Resource Groups，以及可以使用标签编辑器标记的资源类型。

Important

基于所有受支持的资源类型查询的资源组可能会随着时间的推移自动添加成员，因为 Resource Groups 支持新资源。在对基于所有受支持的资源类型的现有资源组运行自动化或其他批量任务时，请注意，运行这些操作的资源可能比首次创建该组时包含的资源多得多。这也可能意味着您为其他资源创建的自动化或任务会应用于可能意想不到的资源或无法成功完成任务的资源。在这种情况下，您可以添加资源类型筛选器来指定只有指定类型的资源才能成为该组的一部分。



下表列出了支持在标签编辑器中添加标签、基于标签查询的群组的成员资格以及基于 AWS CloudFormation 堆栈的群组中的成员资格的资源类型。

列定义

- 标签编辑器标记 -您 可以使用标签编辑器控制台为此类型资源添加标签。否则，您必须使用该资源所拥有服务原生支持的 AWS Resource Groups Tagging API 或标记服务。
- 基于标签的组 - 您可以将此类资源包含在资源组中，其成员资格由附加到资源的标签决定。该组指定标签键的名称和值，任何标签匹配的资源都将自动成为该组的一部分
- AWS CloudFormation 基于堆栈的组-您可以将此类资源包含在资源组中，其成员资格由作为堆栈的一部分创建的资源组成。 CloudFormation 该组指定堆栈的 ARN，其所有资源都自动成为该组的成员。向 AWS CloudFormation 堆栈添加标签会导致堆栈更新。

有关 Resource Groups 已弃用且不再支持的资源类型列表，请参阅本主题末尾的 已弃用的资源类型 部分。

> **Note**
>
> Resource Groups 和标签编辑器支持下表中的资源类型，但有些资源类型可能在您的中不可用 AWS 区域。

Amazon API Gateway

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::ApiGateway::Account	✗ 否	✗ 否	✓ 是
AWS::ApiGateway::ApiKey	✗ 否	✓ 是	✓ 是
AWS::ApiGateway::ClientCertificate	✗ 否	✓ 是	✗ 否
AWS::ApiGateway::DomainName	✗ 否	✗ 否	✓ 是
AWS::ApiGateway::RestApi	✗ 否	✓ 是	✓ 是
AWS::ApiGateway::Stage	✗ 否	✓ 是	✗ 否

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::ApiGateway::UsagePlan	✗ 否	✓ 是	✓ 是

Amazon API Gateway V2

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::ApiGatewayV2::Api	✗ 否	✓ 是	✗ 否

IAM Access Analyzer

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::AccessAnalyzer::Analyzer	✗ 否	✓ 是	✗ 否

AWS Amplify

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Amplify::App	✗ 否	✓ 是	✗ 否

AWS App Mesh

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::AppMesh::Mesh	✗ 否	✓ 是	✗ 否

Amazon AppStream

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::AppStream::AppBlock	✗ 否	✓ 是	✗ 否
AWS::AppStream::Application	✗ 否	✓ 是	✗ 否
AWS::AppStream::Fleet	✓ 是	✓ 是	✓ 是
AWS::AppStream::ImageBuilder	✓ 是	✓ 是	✓ 是
AWS::AppStream::Stack	✓ 是	✓ 是	✓ 是

AWS AppSync

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::AppSync::DataSource	✗ 否	✗ 否	✓ 是

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::AppSync::GraphQLApi	✗ 否	✗ 否	✓ 是

Amazon Athena

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Athena::DataCatalog	✗ 否	✓ 是	✗ 否
AWS::Athena::WorkGroup	✗ 否	✓ 是	✗ 否

AWS Backup

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Backup::BackupPlan	✗ 否	✓ 是	✗ 否
AWS::Backup::BackupVault	✗ 否	✓ 是	✗ 否
AWS::Backup::ReportPlan	✗ 否	✓ 是	✗ 否

AWS Batch

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Batch::ComputeEnvironment	✗ 否	✓ 是	✗ 否
AWS::Batch::JobQueue	✗ 否	✓ 是	✗ 否
AWS::Batch::SchedulingPolicy	✗ 否	✓ 是	✗ 否

AWS Billing Conductor

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::BillingConductor::BillingGroup	✗ 否	✓ 是	✓ 是
AWS::BillingConductor::CustomLineItem	✗ 否	✓ 是	✓ 是
AWS::BillingConductor::PricingPlan	✗ 否	✓ 是	✓ 是
AWS::BillingConductor::PricingRule	✗ 否	✓ 是	✓ 是

Amazon Braket

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Braket::Job	✗ 否	✓ 是	✗ 否
AWS::Braket::QuantumTask	✓ 是	✓ 是	✗ 否

AWS Certificate Manager

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::CertificateManager::Certificate	✓ 是	✓ 是	✓ 是

AWS Certificate Manager 私有证书颁发机构

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::ACMPCA::CertificateAuthority	✗ 否	✓ 是	✗ 否

AWS Cloud9

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Cloud9::Environment	✓ 是	✓ 是	X 否

AWS CloudFormation

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::CloudFormation::Stack	✓ 是	✓ 是	✓ 是

Amazon CloudFront

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::CloudFront::Distribution	✓ 是[1]	✓ 是[2]	✓ 是[2]
AWS::CloudFront::StreamingDistribution	✓ 是[1]	✓ 是[2]	✓ 是[2]

[1] 这是在美国东部（弗吉尼亚北部）区域托管的全球服务的资源。要使用标签编辑器为该资源类型创建或修改标签，您必须在标签编辑器控制台中查找要标记的资源下方的选择区域列表中包含 us-east-1。

[2] 这是在美国东部（弗吉尼亚北部）区域托管的全球服务的资源。由于 Resource Groups 是针对每个区域单独维护的 AWS 区域 ，因此您必须 AWS Management Console 将资源组切换到包含要包含在组中的资源的。要创建包含全球资源的资源组，必须使用右上角的区域选择器 AWS Management Console 将您的资源组配置为美国东部（弗吉尼亚北部）us-east-1。 AWS Management Console

AWS Cloud Map

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::ServiceDiscovery::Service	✗ 否	✓ 是	✗ 否

AWS CloudTrail

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::CloudTrail::Channel	✗ 否	✓ 是	✗ 否
AWS::CloudTrail::EventDataStore	✗ 否	✓ 是	✗ 否
AWS::CloudTrail::Trail	✓ 是	✓ 是	✓ 是

Amazon CloudWatch

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::CloudWatch::Alarm	✓ 是	✓ 是	✓ 是

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::CloudWatch::Dashboard	✗ 否	✗ 否	✓ 是
AWS::CloudWatch::InsightRule	✗ 否	✓ 是	✗ 否
AWS::CloudWatch::MetricStream	✗ 否	✓ 是	✗ 否
AWS::CloudWatch::ServiceLevelObjective	✗ 否	✓ 是	✗ 否

Amazon CloudWatch 日志

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Logs::Destination	✗ 否	✓ 是	✗ 否
AWS::Logs::LogGroup	✗ 否	✓ 是	✓ 是

Amazon S CloudWatch ynthetics

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Synthetics::Canary	✗ 否	✓ 是	✓ 是

AWS CodeArtifact

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::CodeArtifact::Domain	✓ 是	✓ 是	✓ 是
AWS::CodeArtifact::Repository	✓ 是	✓ 是	✓ 是

AWS CodeBuild

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::CodeBuild::Project	✓ 是	✓ 是	X 否

AWS CodeCommit

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::CodeCommit::Repository	✓ 是	✓ 是	X 否

AWS CodeDeploy

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::CodeDeploy::Application	✗ 否	✓ 是	✓ 是
AWS::CodeDeploy::DeploymentConfig	✗ 否	✗ 否	✓ 是

Amazon CodeGuru Reviewer

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::CodeGuruReviewer::RepositoryAssociation	✓ 是	✓ 是	✓ 是

Amazon P CodeGuru rofiler

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::CodeGuruProfiler::ProfilingGroup	✗ 否	✓ 是	✗ 否

AWS CodePipeline

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::CodePipeline::CustomActionType	✗ 否	✓ 是	✗ 否
AWS::CodePipeline::Pipeline	✓ 是	✓ 是	✓ 是
AWS::CodePipeline::Webhook	✓ 是	✓ 是	✓ 是

AWS CodeConnections

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::CodeStarConnections::Connection	✗ 否	✓ 是	✗ 否

Amazon Cognito

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Cognito::IdentityPool	✓ 是	✓ 是	✓ 是
AWS::Cognito::UserPool	✓ 是	✓ 是	✓ 是

Amazon Comprehend

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Comprehend::DocumentClassifier	✓ 是	✓ 是	X 否
AWS::Comprehend::EntityRecognizer	✓ 是	✓ 是	X 否

AWS Config

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Config::AggregationAuthorization	X 否	✓ 是	X 否
AWS::Config::ConfigRule	✓ 是	✓ 是	X 否
AWS::Config::ConfigurationAggregator	X 否	✓ 是	X 否
AWS::Config::StoredQuery	X 否	✓ 是	X 否

Amazon Connect

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Connect::Instance	X 否	✓ 是	X 否

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Connect::PhoneNumber	✗ 否	✓ 是	✗ 否

Amazon Connect Wisdom

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Wisdom::Assistant	✗ 否	✓ 是	✓ 是
AWS::Wisdom::AssistantAssociation	✗ 否	✓ 是	✓ 是
AWS::Wisdom::Content	✗ 否	✓ 是	✗ 否
AWS::Wisdom::KnowledgeBase	✗ 否	✓ 是	✓ 是
AWS::Wisdom::Session	✗ 否	✓ 是	✗ 否

AWS Data Exchange

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::DataExchange::DataSet	✓ 是	✓ 是	✗ 否
AWS::DataExchange::Revision	✗ 否	✓ 是	✗ 否

AWS Data Pipeline

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::DataPipeline::Pipeline	✓ 是	✓ 是	✓ 是

AWS DataSync

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::DataSync::Task	✗ 否	✓ 是	✗ 否

AWS Database Migration Service

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::DMS::Certificate	✓ 是	✓ 是	✗ 否
AWS::DMS::Endpoint	✓ 是	✓ 是	✓ 是
AWS::DMS::EventSubscription	✓ 是	✓ 是	✗ 否
AWS::DMS::ReplicationInstance	✓ 是	✓ 是	✓ 是
AWS::DMS::ReplicationSubnetGroup	✓ 是	✓ 是	✗ 否

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::DMS::ReplicationTask	✓ 是	✓ 是	X 否

AWS Device Farm

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::DeviceFarm::InstanceProfile	X 否	✓ 是	X 否
AWS::DeviceFarm::Project	X 否	✓ 是	X 否
AWS::DeviceFarm::TestGridProject	X 否	✓ 是	X 否

Amazon DynamoDB

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::DynamoDB::Table	✓ 是	✓ 是	✓ 是

Amazon EMR

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::EMR::Cluster	✓ 是	✓ 是	✓ 是

Amazon EMR 容器

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::EMRContainers::JobRun	X 否	✓ 是	X 否
AWS::EMRContainers::VirtualCluster	✓ 是	✓ 是	✓ 是

Amazon EMR Serverless

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::EMRServerless::Application	X 否	✓ 是	✓ 是
AWS::EMRServerless::JobRun	X 否	✓ 是	X 否

Amazon ElastiCache

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::ElastiCache::CacheCluster	✓ 是	✓ 是	✓ 是
AWS::ElastiCache::ParameterGroup	X 否	✓ 是	X 否
AWS::ElastiCache::SecurityGroup	X 否	✓ 是	X 否
AWS::ElastiCache::Snapshot	✓ 是	✓ 是	X 否
AWS::ElastiCache::SubnetGroup	X 否	✓ 是	X 否
AWS::ElastiCache::User	X 否	✓ 是	X 否
AWS::ElastiCache::UserGroup	X 否	✓ 是	X 否

AWS Elastic Beanstalk

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::ElasticBeanstalk::Application	✓ 是	✓ 是	X 否
AWS::ElasticBeanstalk::ApplicationVersion	X 否	✓ 是	X 否
AWS::ElasticBeanstalk::ConfigurationTemplate	X 否	✓ 是	X 否
AWS::ElasticBeanstalk::Environment	X 否	✓ 是	X 否

Amazon Elastic Compute Cloud (Amazon EC2)

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::EC2::CapacityReservation	✗ 否	✓ 是	✗ 否
AWS::EC2::CapacityReservationFleet	✗ 否	✓ 是	✗ 否
AWS::EC2::CarrierGateway	✗ 否	✓ 是	✗ 否
AWS::EC2::ClientVpnEndpoint	✗ 否	✓ 是	✗ 否
AWS::EC2::CoipPool	✗ 否	✓ 是	✗ 否
AWS::EC2::CustomerGateway	✓ 是	✓ 是	✓ 是
AWS::EC2::DHCPOptions	✓ 是	✓ 是	✓ 是
AWS::EC2::EC2Fleet	✗ 否	✓ 是	✗ 否
AWS::EC2::EgressOnlyInternetGateway	✗ 否	✓ 是	✗ 否
AWS::EC2::EIP	✓ 是	✓ 是	✗ 否
AWS::EC2::ExportImageTask	✗ 否	✓ 是	✗ 否
AWS::EC2::ExportInstanceTask	✗ 否	✓ 是	✗ 否
AWS::EC2::FlowLog	✗ 否	✓ 是	✗ 否
AWS::EC2::FpgaImage	✗ 否	✓ 是	✗ 否
AWS::EC2::Host	✗ 否	✓ 是	✗ 否
AWS::EC2::HostReservation	✗ 否	✓ 是	✗ 否
AWS::EC2::Image	✓ 是	✓ 是	✗ 否

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::EC2::ImportImageTask	✗ 否	✓ 是	✗ 否
AWS::EC2::ImportSnapshotTask	✗ 否	✓ 是	✗ 否
AWS::EC2::Instance	✓ 是	✓ 是	✓ 是
AWS::EC2::InstanceEventWindow	✗ 否	✓ 是	✗ 否
AWS::EC2::InternetGateway	✓ 是	✓ 是	✓ 是
AWS::EC2::IPv4Pool	✗ 否	✓ 是	✗ 否
AWS::EC2::IPv6Pool	✗ 否	✓ 是	✗ 否
AWS::EC2::KeyPair	✗ 否	✓ 是	✗ 否
AWS::EC2::LaunchTemplate	✗ 否	✓ 是	✓ 是
AWS::EC2::LocalGateway	✗ 否	✓ 是	✗ 否
AWS::EC2::LocalGatewayRouteTable	✗ 否	✓ 是	✗ 否
AWS::EC2::LocalGatewayRouteTableVirtualInterfaceGroupAssociation	✗ 否	✓ 是	✗ 否
AWS::EC2::LocalGatewayRouteTableVPCAssociation	✗ 否	✓ 是	✗ 否
AWS::EC2::LocalGatewayVirtualInterface	✗ 否	✓ 是	✗ 否
AWS::EC2::LocalGatewayVirtualInterfaceGroup	✗ 否	✓ 是	✗ 否
AWS::EC2::NatGateway	✓ 是	✓ 是	✓ 是

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::EC2::NetworkAcl	✓ 是	✓ 是	✓ 是
AWS::EC2::NetworkInsightsAccessScope	✗ 否	✓ 是	✗ 否
AWS::EC2::NetworkInsightsAccessScopeAnalysis	✗ 否	✓ 是	✗ 否
AWS::EC2::NetworkInsightsAnalysis	✗ 否	✓ 是	✗ 否
AWS::EC2::NetworkInsightsPath	✗ 否	✓ 是	✗ 否
AWS::EC2::NetworkInterface	✓ 是	✓ 是	✓ 是
AWS::EC2::PlacementGroup	✗ 否	✓ 是	✓ 是
AWS::EC2::PrefixList	✗ 否	✓ 是	✗ 否
AWS::EC2::ReplaceRootVolumeTask	✗ 否	✓ 是	✗ 否
AWS::EC2::ReservedInstance	✓ 是	✓ 是	✗ 否
AWS::EC2::RouteTable	✓ 是	✓ 是	✓ 是
AWS::EC2::SecurityGroup	✓ 是	✓ 是	✓ 是
AWS::EC2::Snapshot	✓ 是	✓ 是	✗ 否
AWS::EC2::SpotFleet	✗ 否	✓ 是	✗ 否
AWS::EC2::SpotInstanceRequest	✓ 是	✓ 是	✗ 否
AWS::EC2::Subnet	✓ 是	✓ 是	✓ 是
AWS::EC2::SubnetCidrReservation	✗ 否	✓ 是	✗ 否
AWS::EC2::TrafficMirrorFilter	✗ 否	✓ 是	✗ 否

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::EC2::TrafficMirrorSession	✗ 否	✓ 是	✗ 否
AWS::EC2::TrafficMirrorTarget	✗ 否	✓ 是	✗ 否
AWS::EC2::TransitGateway	✗ 否	✓ 是	✗ 否
AWS::EC2::TransitGatewayAttachment	✗ 否	✓ 是	✗ 否
AWS::EC2::TransitGatewayConnectPeer	✗ 否	✓ 是	✗ 否
AWS::EC2::TransitGatewayMulticastDomain	✗ 否	✓ 是	✗ 否
AWS::EC2::TransitGatewayPolicyTable	✗ 否	✓ 是	✗ 否
AWS::EC2::TransitGatewayRouteTable	✗ 否	✓ 是	✗ 否
AWS::EC2::TransitGatewayRouteTableAnnouncement	✗ 否	✓ 是	✗ 否
AWS::EC2::VerifiedAccessEndpoint	✗ 否	✓ 是	✗ 否
AWS::EC2::VerifiedAccessGroup	✗ 否	✓ 是	✗ 否
AWS::EC2::VerifiedAccessInstance	✗ 否	✓ 是	✗ 否
AWS::EC2::VerifiedAccessTrustProvider	✗ 否	✓ 是	✗ 否
AWS::EC2::Volume	✓ 是	✓ 是	✓ 是
AWS::EC2::VPC	✓ 是	✓ 是	✓ 是
AWS::EC2::VPCEndpoint	✗ 否	✓ 是	✗ 否
AWS::EC2::VPCEndpointConnection	✗ 否	✓ 是	✗ 否

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::EC2::VPCEndpointService	✗ 否	✓ 是	✗ 否
AWS::EC2::VPCEndpointServicePermissions	✗ 否	✓ 是	✗ 否
AWS::EC2::VPCPeeringConnection	✗ 否	✓ 是	✓ 是
AWS::EC2::VPNConnection	✓ 是	✓ 是	✓ 是
AWS::EC2::VPNGateway	✓ 是	✓ 是	✓ 是

Amazon Elastic Container Registry

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::ECR::Repository	✗ 否	✓ 是	✗ 否

Amazon Elastic Container Service

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::ECS::CapacityProvider	✗ 否	✓ 是	✗ 否
AWS::ECS::Cluster	✓ 是	✓ 是	✗ 否

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::ECS::ContainerInstance	✗ 否	✓ 是	✗ 否
AWS::ECS::Service	✗ 否	✓ 是	✗ 否
AWS::ECS::Task	✗ 否	✓ 是	✗ 否
AWS::ECS::TaskDefinition	✓ 是	✓ 是	✗ 否
AWS::ECS::TaskSet	✗ 否	✓ 是	✗ 否

Amazon Elastic File System

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::EFS::FileSystem	✓ 是	✓ 是	✓ 是

Amazon Elastic Inference

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::ElasticInference::ElasticInferenceAccelerator	✓ 是	✓ 是	✗ 否

Amazon Elastic Kubernetes Service(Amazon EKS)

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::EKS::Addon	✗ 否	✓ 是	✗ 否
AWS::EKS::Cluster	✓ 是	✓ 是	✓ 是

Elastic Load Balancing

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::ElasticLoadBalancing::LoadBalancer	✓ 是	✓ 是	✓ 是
AWS::ElasticLoadBalancingV2::Listener	✗ 否	✓ 是	✓ 是
AWS::ElasticLoadBalancingV2::ListenerRule	✗ 否	✓ 是	✓ 是
AWS::ElasticLoadBalancingV2::LoadBalancer	✓ 是	✓ 是	✓ 是
AWS::ElasticLoadBalancingV2::TargetGroup	✓ 是	✓ 是	✓ 是

亚马逊 OpenSearch 服务

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Elasticsearch::Domain	✓ 是	✓ 是	✓ 是

亚马逊 CloudWatch 活动

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Events::EventBus	X 否	✓ 是	X 否
AWS::Events::Rule	✓ 是	✓ 是	✓ 是

> **Note**
>
> 标签编辑器不支持自定义事件总线中的规则。

亚马逊 EventBridge 架构

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::EventSchemas::Discoverer	X 否	✓ 是	X 否

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::EventSchemas::Registry	✗ 否	✓ 是	✗ 否
AWS::EventSchemas::Schema	✗ 否	✓ 是	✗ 否

Amazon FSx

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::FSx::FileSystem	✓ 是	✓ 是	✗ 否
AWS::FSx::StorageVirtualMachine	✗ 否	✓ 是	✗ 否
AWS::FSx::Volume	✗ 否	✓ 是	✗ 否

Amazon Forecast

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Forecast::Dataset	✓ 是	✓ 是	✗ 否
AWS::Forecast::DatasetGroup	✓ 是	✓ 是	✗ 否
AWS::Forecast::DatasetImportJob	✓ 是	✓ 是	✗ 否
AWS::Forecast::Forecast	✓ 是	✓ 是	✗ 否

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Forecast::ForecastExportJob	✓ 是	✓ 是	X 否
AWS::Forecast::Predictor	✓ 是	✓ 是	X 否
AWS::Forecast::PredictorBacktestExportJob	✓ 是	✓ 是	X 否

Amazon Fraud Detector

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::FraudDetector::Detector	✓ 是	✓ 是	X 否
AWS::FraudDetector::DetectorVersion	X 否	✓ 是	X 否
AWS::FraudDetector::EntityType	✓ 是	✓ 是	X 否
AWS::FraudDetector::EventType	✓ 是	✓ 是	X 否
AWS::FraudDetector::ExternalModel	✓ 是	✓ 是	X 否
AWS::FraudDetector::Label	✓ 是	✓ 是	X 否
AWS::FraudDetector::Model	✓ 是	✓ 是	X 否
AWS::FraudDetector::ModelVersion	X 否	✓ 是	X 否
AWS::FraudDetector::Outcome	✓ 是	✓ 是	X 否
AWS::FraudDetector::Rule	X 否	✓ 是	X 否

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::FraudDetector::Variable	✓ 是	✓ 是	X 否

Amazon GameLift

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::GameLift::Alias	X 否	✓ 是	X 否
AWS::GameLift::GameSessionQueue	X 否	✓ 是	X 否
AWS::GameLift::Location	X 否	✓ 是	X 否
AWS::GameLift::MatchmakingConfiguration	X 否	✓ 是	X 否
AWS::GameLift::MatchmakingRuleSet	X 否	✓ 是	X 否

AWS Global Accelerator

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::GlobalAccelerator::Accelerator	X 否	✓ 是	X 否

AWS Glue

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Glue::Crawler	✓ 是	✓ 是	× 否
AWS::Glue::Database	× 否	✓ 是	✓ 是
AWS::Glue::Job	✓ 是	✓ 是	× 否
AWS::Glue::MLTransform	× 否	✓ 是	× 否
AWS::Glue::Registry	× 否	✓ 是	× 否
AWS::Glue::Trigger	✓ 是	✓ 是	× 否
AWS::Glue::Workflow	× 否	✓ 是	× 否

AWS Glue DataBrew

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::DataBrew::Dataset	✓ 是	✓ 是	✓ 是
AWS::DataBrew::Job	✓ 是	✓ 是	✓ 是
AWS::DataBrew::Project	✓ 是	✓ 是	✓ 是
AWS::DataBrew::Recipe	✓ 是	✓ 是	✓ 是
AWS::DataBrew::Schedule	✓ 是	✓ 是	✓ 是

AWS Ground Station

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::GroundStation::Config	✗ 否	✓ 是	✗ 否
AWS::GroundStation::DataflowEndpointGroup	✗ 否	✓ 是	✗ 否
AWS::GroundStation::MissionProfile	✗ 否	✓ 是	✗ 否

Amazon GuardDuty

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::GuardDuty::Detector	✗ 否	✓ 是	✓ 是
AWS::GuardDuty::Filter	✗ 否	✓ 是	✗ 否
AWS::GuardDuty::IPSet	✗ 否	✓ 是	✗ 否
AWS::GuardDuty::ThreatIntelSet	✗ 否	✓ 是	✗ 否

Amazon Interactive Video Service

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::IVS::Channel	✗ 否	✓ 是	✗ 否
AWS::IVS::RecordingConfiguration	✗ 否	✓ 是	✗ 否
AWS::IVS::StreamKey	✗ 否	✓ 是	✗ 否

AWS Identity and Access Management

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::IAM::InstanceProfile	✓ 是[1]	✓ 是[2]	✗ 否
AWS::IAM::ManagedPolicy	✓ 是[1]	✓ 是[2]	✗ 否
AWS::IAM::OpenIDConnectProvider	✓ 是[1]	✓ 是[2]	✗ 否
AWS::IAM::Role	✗ 否	✗ 否	✓ 是[2]
AWS::IAM::SAMLProvider	✓ 是[1]	✓ 是[2]	✗ 否
AWS::IAM::ServerCertificate	✓ 是[1]	✓ 是[2]	✗ 否
AWS::IAM::VirtualMFADevice	✓ 是[1]	✓ 是[2]	✗ 否

[1] 这是在美国东部（弗吉尼亚北部）区域托管的全球服务的资源。要使用标签编辑器为该资源类型创建或修改标签，您必须在标签编辑器控制台中查找要标记的资源下方的选择区域列表中包含 us-east-1。

[2] 这是在美国东部（弗吉尼亚北部）区域托管的全球服务的资源。由于 Resource Groups 是针对每个区域单独维护的 AWS 区域 ，因此您必须 AWS Management Console 将资源组切换到包含要包含在组中的资源的。要创建包含全球资源的资源组，必须使用右上角的区域选择器 AWS Management Console 将您的资源组配置为美国东部（弗吉尼亚北部）us-east-1。 AWS Management Console

EC2 Image Builder

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::ImageBuilder::Component	✗ 否	✓ 是	✗ 否
AWS::ImageBuilder::ContainerRecipe	✗ 否	✓ 是	✗ 否
AWS::ImageBuilder::DistributionConfiguration	✗ 否	✓ 是	✗ 否
AWS::ImageBuilder::Image	✗ 否	✓ 是	✗ 否
AWS::ImageBuilder::ImagePipeline	✗ 否	✓ 是	✗ 否
AWS::ImageBuilder::ImageRecipe	✗ 否	✓ 是	✗ 否
AWS::ImageBuilder::InfrastructureConfiguration	✗ 否	✓ 是	✗ 否

Amazon Inspector

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Inspector::AssessmentTemplate	✗ 否	✓ 是	✓ 是

AWS IoT

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::IoT::Authorizer	✗ 否	✓ 是	✗ 否
AWS::IoT::BillingGroup	✗ 否	✓ 是	✗ 否
AWS::IoT::CACertificate	✗ 否	✓ 是	✗ 否
AWS::IoT::CustomMetric	✗ 否	✓ 是	✗ 否
AWS::IoT::Dimension	✗ 否	✓ 是	✗ 否
AWS::IoT::JobTemplate	✗ 否	✓ 是	✗ 否
AWS::IoT::MitigationAction	✗ 否	✓ 是	✗ 否
AWS::IoT::Policy	✗ 否	✓ 是	✗ 否
AWS::IoT::RoleAlias	✗ 否	✓ 是	✗ 否
AWS::IoT::ScheduledAudit	✗ 否	✓ 是	✗ 否
AWS::IoT::SecurityProfile	✗ 否	✓ 是	✗ 否
AWS::IoT::ThingGroup	✗ 否	✓ 是	✗ 否
AWS::IoT::ThingType	✗ 否	✓ 是	✗ 否
AWS::IoT::TopicRule	✗ 否	✓ 是	✓ 是

AWS IoT Analytics

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::IoTAnalytics::Channel	✗ 否	✓ 是	✗ 否
AWS::IoTAnalytics::Dataset	✓ 是	✓ 是	✗ 否
AWS::IoTAnalytics::Datastore	✗ 否	✓ 是	✗ 否
AWS::IoTAnalytics::Pipeline	✗ 否	✓ 是	✗ 否

AWS IoT Events

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::IoTEvents::AlarmModel	✗ 否	✓ 是	✗ 否
AWS::IoTEvents::DetectorModel	✓ 是	✓ 是	✓ 是
AWS::IoTEvents::Input	✓ 是	✓ 是	✓ 是

AWS IoT FleetWise

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::IoTFleetWise::Campaign	✗ 否	✓ 是	✓ 是
AWS::IoTFleetWise::DecoderManifest	✗ 否	✓ 是	✓ 是
AWS::IoTFleetWise::Fleet	✗ 否	✓ 是	✓ 是
AWS::IoTFleetWise::ModelManifest	✗ 否	✓ 是	✓ 是
AWS::IoTFleetWise::SignalCatalog	✗ 否	✓ 是	✓ 是
AWS::IoTFleetWise::Vehicle	✗ 否	✓ 是	✓ 是

AWS IoT Greengrass

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Greengrass::ConnectorDefinition	✓ 是	✓ 是	✗ 否
AWS::Greengrass::CoreDefinition	✓ 是	✓ 是	✗ 否
AWS::Greengrass::DeviceDefinition	✓ 是	✓ 是	✗ 否
AWS::Greengrass::FunctionDefinition	✓ 是	✓ 是	✗ 否
AWS::Greengrass::Group	✓ 是	✓ 是	✗ 否
AWS::Greengrass::LoggerDefinition	✓ 是	✓ 是	✗ 否

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Greengrass::ResourceDefinition	✓ 是	✓ 是	X 否
AWS::Greengrass::SubscriptionDefinition	✓ 是	✓ 是	X 否

AWS IoT Greengrass Version 2

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::GreengrassV2::ComponentVersion	X 否	✓ 是	X 否

AWS IoT SiteWise 控制台

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::IoTSiteWise::Asset	X 否	✓ 是	X 否
AWS::IoTSiteWise::AssetModel	X 否	✓ 是	X 否
AWS::IoTSiteWise::Dashboard	X 否	✓ 是	X 否
AWS::IoTSiteWise::Gateway	X 否	✓ 是	X 否
AWS::IoTSiteWise::Portal	X 否	✓ 是	X 否

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::IoTSiteWise::Project	✗ 否	✓ 是	✗ 否

AWS IoT Wireless

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::IoTWireless::Destination	✗ 否	✓ 是	✗ 否
AWS::IoTWireless::DeviceProfile	✗ 否	✓ 是	✗ 否
AWS::IoTWireless::FuotaTask	✗ 否	✓ 是	✗ 否
AWS::IoTWireless::MulticastGroup	✗ 否	✓ 是	✗ 否
AWS::IoTWireless::NetworkAnalyzerConfiguration	✗ 否	✓ 是	✗ 否
AWS::IoTWireless::ServiceProfile	✗ 否	✓ 是	✗ 否
AWS::IoTWireless::TaskDefinition	✗ 否	✓ 是	✗ 否
AWS::IoTWireless::WirelessDevice	✗ 否	✓ 是	✗ 否
AWS::IoTWireless::WirelessGateway	✗ 否	✓ 是	✗ 否

AWS Key Management Service

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::KMS::Alias	✗ 否	✗ 否	✓ 是
AWS::KMS::Key	✓ 是	✓ 是	✓ 是

Amazon Keyspaces（Apache Cassandra 兼容）

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Cassandra::Keyspace	✗ 否	✓ 是	✓ 是
AWS::Cassandra::Table	✗ 否	✓ 是	✗ 否

Amazon Kinesis

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Kinesis::Stream	✓ 是	✓ 是	✓ 是

适用于 Apache Flink 的亚马逊托管服务

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::KinesisAnalytics::Application	✓ 是	✓ 是	✓ 是
AWS::KinesisAnalyticsV2::Application	X 否	X 否	✓ 是

Amazon Data Firehose

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::KinesisFirehose::DeliveryStream	X 否	✓ 是	✓ 是

AWS Lambda

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Lambda::Alias	X 否	X 否	✓ 是
AWS::Lambda::EventSourceMapping	X 否	X 否	✓ 是
AWS::Lambda::Function	✓ 是	✓ 是	✓ 是
AWS::Lambda::LayerVersion	X 否	X 否	✓ 是

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Lambda::Version	✗ 否	✗ 否	✓ 是

Amazon Lightsail

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Lightsail::Bucket	✗ 否	✓ 是	✗ 否
AWS::Lightsail::Certificate	✗ 否	✓ 是	✗ 否
AWS::Lightsail::Container	✗ 否	✓ 是	✗ 否
AWS::Lightsail::Disk	✗ 否	✓ 是	✗ 否
AWS::Lightsail::Distribution	✗ 否	✓ 是	✗ 否
AWS::Lightsail::Instance	✗ 否	✓ 是	✗ 否
AWS::Lightsail::StaticIp	✗ 否	✓ 是	✗ 否

Amazon MQ

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::AmazonMQ::Broker	✓ 是	✓ 是	✗ 否

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::AmazonMQ::Configuration	✓ 是	✓ 是	X 否

Amazon Macie

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Macie::ClassificationJob	✓ 是	✓ 是	X 否
AWS::Macie::CustomDataIdentifier	✓ 是	✓ 是	✓ 是
AWS::Macie::FindingsFilter	✓ 是	✓ 是	✓ 是
AWS::Macie::Member	✓ 是	✓ 是	X 否

Amazon Managed Blockchain

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::ManagedBlockchain::Accessor	X 否	✓ 是	X 否

Amazon Managed Streaming for Apache Kafka

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Kafka::Cluster	✓ 是	✓ 是	X 否

AWS Elemental MediaConnect

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::MediaConnect::Flow	X 否	✓ 是	X 否
AWS::MediaConnect::FlowEntitlement	X 否	✓ 是	X 否
AWS::MediaConnect::FlowOutput	X 否	✓ 是	X 否
AWS::MediaConnect::FlowSource	X 否	✓ 是	X 否

AWS Elemental MediaPackage

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::MediaPackage::Channel	X 否	✓ 是	X 否
AWS::MediaPackage::PackagingConfiguration	X 否	✓ 是	X 否

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::MediaPackage::PackagingGroup	✗ 否	✓ 是	✗ 否

AWS Network Manager

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::NetworkManager::CoreNetwork	✗ 否	✓ 是	✗ 否
AWS::NetworkManager::Device	✗ 否	✓ 是	✗ 否
AWS::NetworkManager::GlobalNetwork	✗ 否	✓ 是	✗ 否
AWS::NetworkManager::Link	✗ 否	✓ 是	✗ 否
AWS::NetworkManager::Site	✗ 否	✓ 是	✗ 否
AWS::NetworkManager::VpcAttachment	✗ 否	✓ 是	✗ 否

亚马逊 OpenSearch 服务 OpenSearch

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::OpenSearchService::Domain	✓ 是	✓ 是	✓ 是

AWS OpsWorks

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::OpsWorks::Instance	✗ 否	✓ 是	✓ 是
AWS::OpsWorks::Layer	✗ 否	✓ 是	✓ 是
AWS::OpsWorks::Stack	✗ 否	✓ 是	✓ 是

AWS Organizations

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Organizations::Account	✓ 是	✓ 是	✗ 否
AWS::Organizations::OrganizationalUnit	✗ 否	✓ 是	✗ 否
AWS::Organizations::Policy	✗ 否	✓ 是	✗ 否
AWS::Organizations::Root	✓ 是	✓ 是	✗ 否

Amazon Pinpoint

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Pinpoint::App	✗ 否	✓ 是	✓ 是
AWS::Pinpoint::EmailTemplate	✗ 否	✓ 是	✓ 是
AWS::Pinpoint::PushTemplate	✗ 否	✓ 是	✓ 是
AWS::Pinpoint::SmsTemplate	✗ 否	✓ 是	✓ 是
AWS::Pinpoint::VoiceTemplate	✗ 否	✓ 是	✗ 否

Amazon Pinpoint 短信和语音 API

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::PinpointSMSVoiceV2::Pool	✗ 否	✓ 是	✗ 否

Amazon Quantum Ledger Database (Amazon QLDB)

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::QLDB::Ledger	✓ 是	✓ 是	✓ 是

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::QLDB::Stream	✗ 否	✓ 是	✓ 是

Amazon Redshift

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Redshift::Cluster	✓ 是	✓ 是	✓ 是
AWS::Redshift::ClusterParameterGroup	✓ 是	✓ 是	✓ 是
AWS::Redshift::ClusterSecurityGroup	✗ 否	✓ 是	✓ 是
AWS::Redshift::ClusterSubnetGroup	✓ 是	✓ 是	✓ 是
AWS::Redshift::DBGroup	✗ 否	✓ 是	✗ 否
AWS::Redshift::DBName	✗ 否	✓ 是	✗ 否
AWS::Redshift::DBUser	✗ 否	✓ 是	✗ 否
AWS::Redshift::EventSubscription	✗ 否	✓ 是	✗ 否
AWS::Redshift::HSMClientCertificate	✓ 是	✓ 是	✗ 否
AWS::Redshift::HSMConfiguration	✗ 否	✓ 是	✗ 否
AWS::Redshift::Namespace	✗ 否	✓ 是	✗ 否
AWS::Redshift::Snapshot	✗ 否	✓ 是	✗ 否
AWS::Redshift::SnapshotCopyGrant	✗ 否	✓ 是	✗ 否

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Redshift::SnapshotSchedule	✗ 否	✓ 是	✗ 否
AWS::Redshift::UsageLimit	✗ 否	✓ 是	✗ 否

Amazon Relational Database Service (Amazon RDS)

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::RDS::CustomDBEngineVersion	✗ 否	✓ 是	✗ 否
AWS::RDS::DBCluster	✓ 是	✓ 是	✓ 是
AWS::RDS::DBClusterEndpoint	✗ 否	✓ 是	✗ 否
AWS::RDS::DBClusterParameterGroup	✓ 是	✓ 是	✓ 是
AWS::RDS::DBClusterSnapshot	✓ 是	✓ 是	✗ 否
AWS::RDS::DBInstance	✓ 是	✓ 是	✓ 是
AWS::RDS::DBParameterGroup	✓ 是	✓ 是	✓ 是
AWS::RDS::DBProxy	✗ 否	✓ 是	✗ 否
AWS::RDS::DBProxyEndpoint	✗ 否	✓ 是	✗ 否
AWS::RDS::DBProxyTargetGroup	✗ 否	✓ 是	✗ 否
AWS::RDS::DBSecurityGroup	✓ 是	✓ 是	✓ 是
AWS::RDS::DBSnapshot	✓ 是	✓ 是	✗ 否

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::RDS::DBSubnetGroup	✓ 是	✓ 是	✓ 是
AWS::RDS::Deployment	X 否	✓ 是	X 否
AWS::RDS::EventSubscription	✓ 是	✓ 是	X 否
AWS::RDS::OptionGroup	✓ 是	✓ 是	X 否
AWS::RDS::ReservedDBInstance	✓ 是	✓ 是	X 否

AWS Resource Access Manager

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::RAM::ResourceShare	✓ 是	✓ 是	X 否

AWS Resource Groups

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::ResourceGroups::Group	✓ 是	✓ 是	✓ 是

AWS Robomaker

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::RoboMaker::DeploymentJob	✗ 否	✓ 是	✗ 否
AWS::RoboMaker::Fleet	✗ 否	✓ 是	✗ 否
AWS::RoboMaker::Robot	✗ 否	✓ 是	✗ 否
AWS::RoboMaker::RobotApplication	✓ 是	✓ 是	✗ 否
AWS::RoboMaker::SimulationApplication	✓ 是	✓ 是	✗ 否
AWS::RoboMaker::SimulationJob	✓ 是	✓ 是	✗ 否

Amazon Route 53

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Route53::Domain	✓ 是[1]	✓ 是[2]	✗ 否
AWS::Route53::HealthCheck	✓ 是[1]	✓ 是[2]	✓ 是[2]
AWS::Route53::HostedZone	✓ 是[1]	✓ 是[2]	✓ 是[2]

[1] 这是在美国东部（弗吉尼亚北部）区域托管的全球服务的资源。要使用标签编辑器为该资源类型创建或修改标签，您必须在标签编辑器控制台中查找要标记的资源下方的选择区域列表中包含 us-east-1。

[2] 这是在美国东部（弗吉尼亚北部）区域托管的全球服务的资源。由于 Resource Groups 是针对每个区域单独维护的 AWS 区域 ，因此您必须 AWS Management Console 将资源组切换到包含要包含在组中的资源的。要创建包含全球资源的资源组，必须使用右上角的区域选择器 AWS Management Console 将您的资源组配置为美国东部（弗吉尼亚北部）us-east-1。 AWS Management Console

Amazon Route 53 Resolver

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Route53Resolver::FirewallDomainList	✗ 否	✓ 是[2]	✗ 否
AWS::Route53Resolver::FirewallRuleGroup	✗ 否	✓ 是[2]	✗ 否
AWS::Route53Resolver::FirewallRuleGroupAssociation	✗ 否	✓ 是[2]	✗ 否
AWS::Route53Resolver::ResolverEndpoint	✓ 是[1]	✓ 是[2]	✗ 否
AWS::Route53Resolver::ResolverQueryLoggingConfig	✗ 否	✓ 是[2]	✗ 否
AWS::Route53Resolver::ResolverRule	✓ 是[1]	✓ 是[2]	✗ 否

[1] 这是在美国东部（弗吉尼亚北部）区域托管的全球服务的资源。要使用标签编辑器为该资源类型创建或修改标签，您必须在标签编辑器控制台中查找要标记的资源下方的选择区域列表中包含 us-east-1。

[2] 这是在美国东部（弗吉尼亚北部）区域托管的全球服务的资源。由于 Resource Groups 是针对每个区域单独维护的 AWS 区域 ，因此您必须 AWS Management Console 将资源组切换到包含要包含在组中的资源的。要创建包含全球资源的资源组，必须使用右上角的区域选择器 AWS Management Console 将您的资源组配置为美国东部（弗吉尼亚北部）us-east-1。 AWS Management Console

Amazon S3 Glacier

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Glacier::Vault	✓ 是	✓ 是	X 否

Amazon SageMaker

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::SageMaker::AppImageConfig	X 否	✓ 是	X 否
AWS::SageMaker::CodeRepository	X 否	✓ 是	X 否
AWS::SageMaker::Endpoint	X 否	✓ 是	✓ 是
AWS::SageMaker::EndpointConfig	X 否	✓ 是	✓ 是
AWS::SageMaker::HyperParameterTuningJob	X 否	✓ 是	X 否
AWS::SageMaker::Image	X 否	✓ 是	X 否
AWS::SageMaker::LabelingJob	X 否	✓ 是	X 否
AWS::SageMaker::Model	X 否	✓ 是	✓ 是
AWS::SageMaker::ModelPackageGroup	X 否	✓ 是	✓ 是
AWS::SageMaker::NotebookInstance	✓ 是	✓ 是	✓ 是
AWS::SageMaker::Pipeline	X 否	✓ 是	X 否

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::SageMaker::Project	✗ 否	✓ 是	✓ 是
AWS::SageMaker::TrainingJob	✗ 否	✓ 是	✗ 否
AWS::SageMaker::TransformJob	✗ 否	✓ 是	✗ 否
AWS::SageMaker::Workteam	✗ 否	✓ 是	✗ 否

AWS Secrets Manager

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::SecretsManager::Secret	✓ 是	✓ 是	✓ 是

AWS Service Catalog

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::ServiceCatalog::CloudFormationProduct	✗ 否	✓ 是	✓ 是
AWS::ServiceCatalog::Portfolio	✗ 否	✓ 是	✓ 是

AWS Service Catalog AppRegistry

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::ServiceCatalogAppRegistry::Application	✗ 否	✓ 是	✗ 否
AWS::ServiceCatalogAppRegistry::AttributeGroup	✗ 否	✓ 是	✗ 否

服务限额

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::ServiceQuotas::Quota	✗ 否	✓ 是	✗ 否

Amazon Simple Email Service

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::SES::ConfigurationSet	✓ 是	✓ 是	✓ 是
AWS::SES::ContactList	✓ 是	✓ 是	✓ 是
AWS::SES::DedicatedIpPool	✓ 是	✓ 是	✗ 否

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::SES::Identity	✓ 是	✓ 是	✗ 否

Amazon Simple Notification Service

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::SNS::Topic	✓ 是	✓ 是	✓ 是

Amazon Simple Queue Service

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::SQS::Queue	✓ 是	✓ 是	✓ 是

Amazon Simple Storage Service (Amazon S3)

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::S3::Bucket	✓ 是	✓ 是	✓ 是

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::S3::Job	✗ 否	✓ 是	✗ 否
AWS::S3::StorageLens	✗ 否	✓ 是	✗ 否

AWS Step Functions

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::StepFunctions::Activity	✓ 是	✓ 是	✓ 是
AWS::StepFunctions::StateMachine	✓ 是	✓ 是	✓ 是

Storage Gateway

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::StorageGateway::Gateway	✓ 是	✓ 是	✗ 否
AWS::StorageGateway::Volume	✗ 否	✓ 是	✗ 否

AWS Systems Manager

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::SSM::Association	✗ 否	✓ 是	✗ 否
AWS::SSM::AutomationExecution	✗ 否	✓ 是	✗ 否
AWS::SSM::Document	✗ 否	✓ 是	✓ 是
AWS::SSM::MaintenanceWindow	✗ 否	✓ 是	✗ 否
AWS::SSM::ManagedInstance	✗ 否	✓ 是	✗ 否
AWS::SSM::OpsItem	✗ 否	✓ 是	✗ 否
AWS::SSM::OpsMetadata	✗ 否	✓ 是	✗ 否
AWS::SSM::Parameter	✓ 是	✓ 是	✓ 是
AWS::SSM::PatchBaseline	✗ 否	✓ 是	✓ 是

AWS Systems Manager 适用于 SAP

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::SystemsManagerSAP::Application	✗ 否	✓ 是	✓ 是
AWS::SystemsManagerSAP::Database	✗ 否	✓ 是	✗ 否

Amazon Timestream

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Timestream::ScheduledQuery	✗ 否	✓ 是	✓ 是

AWS Transfer Family

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::Transfer::Certificate	✗ 否	✓ 是	✗ 否
AWS::Transfer::Connector	✗ 否	✓ 是	✗ 否
AWS::Transfer::Profile	✗ 否	✓ 是	✗ 否
AWS::Transfer::Workflow	✗ 否	✓ 是	✗ 否

AWS WAF

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::WAF::Rule	✗ 否	✓ 是	✗ 否
AWS::WAF::WebACL	✗ 否	✓ 是	✗ 否

Amazon WorkSpaces

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::WorkSpaces::Workspace	✓ 是	✓ 是	✓ 是

AWS X-Ray

资源	标签编辑器标记	基于标签的组	AWS CloudFormation 基于堆栈的群组
AWS::XRay::Group	X 否	✓ 是	X 否
AWS::XRay::SamplingRule	X 否	✓ 是	X 否

已弃用的资源类型

指定功能不再支持以下资源类型。

服务	资源类型	支持更改	日期
AWS RoboMaker	AWS::RoboMaker::Robot	标签编辑器不再支持。	2022 年 5 月 2 日
AWS RoboMaker	AWS::RoboMaker::Fleet	标签编辑器不再支持。	2022 年 5 月 2 日
AWS RoboMaker	AWS::RoboMaker::DeploymentJob	标签编辑器不再支持。	2022 年 5 月 2 日

使用 AWS CloudFormation创建资源组

AWS Resource Groups 与一项服务集成 AWS CloudFormation，该服务可帮助您对 AWS 资源进行建模和设置，从而减少创建和管理资源和基础架构所花费的时间。您可以创建一个描述所需的所有 AWS 资源（例如资源组）的模板，并为您 AWS CloudFormation 预置和配置这些资源。

使用时 AWS CloudFormation，您可以重复使用模板来一致且重复地设置资源组。描述一次您的资源组，然后在多个 AWS 账户 和区域中一遍又一遍地配置相同的资源组。

Resource Groups 和 AWS CloudFormation 模板

要为 Resource Groups 和相关服务设置和配置资源，您必须了解 AWS CloudFormation 模板。模板是JSON或格式化的文本文件YAML。这些模板描述了您要在 AWS CloudFormation 堆栈中配置的资源。如果您不熟悉JSON或YAML，可以使用 AWS CloudFormation Designer 来帮助您开始使用 AWS CloudFormation 模板。有关更多信息，请参阅什么是 AWS CloudFormation 设计器？ 在《AWS CloudFormation 用户指南》中。

Resource Groups 支持在中创建资源组 AWS CloudFormation。有关更多信息，包括资源组的示例JSON和YAML模板，请参阅AWS CloudFormation 用户指南中的AWS Resource Groups 资源类型参考。

了解更多关于 AWS CloudFormation

要了解更多信息 AWS CloudFormation，请参阅以下资源：

- AWS CloudFormation
- AWS CloudFormation 用户指南
- AWS CloudFormation API参考
- AWS CloudFormation 命令行界面用户指南

AWS Resource Groups 中的安全性

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云中运行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。要了解适用于 AWS Resource Groups 的合规性计划，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。您还需要对其它因素负责，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 Resource Groups 时应用责任共担模式。以下主题说明如何配置 Resource Groups 以实现您的安全性和合规性目标。您还会了解如何使用其他 AWS 服务以帮助您监控和保护 Resource Groups 资源。

主题

中的数据保护 AWS Resource Groups

这些区域有： AWS 分担责任模型适用于以下领域的数据保护 AWS Resource Groups。 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 Resource Groups 或其他资源时 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

与其他相比 AWS 服务， AWS Resource Groups 攻击面最小，因为它不提供更改、添加或删除的方法 AWS 除群组之外的资源。Resource Groups 会向您收集以下特定于服务的信息。

- 组名称（未加密，非私有）
- 组描述（未加密，但为私有）
- 组中的成员资源（这些资源存储在未加密的日志中）

静态加密

没有其他方法可以隔离特定于 Resource Groups 的服务或网络流量。如果适用，请使用 AWS-特异性隔离。您可以使用中的资源组（Resource Groups）API和控制台VPC来帮助最大限度地提高隐私和基础架构安全性。

传输中加密

AWS Resource Groups 数据在传输到服务的内部数据库进行备份时会经过加密。用户无法对其进行配置。

密钥管理

AWS Resource Groups 当前未与集成 AWS Key Management Service 并且不支持 AWS KMS keys.

互联网络流量隐私保护

AWS Resource Groups 用HTTPS于 Resource Groups 用户之间的所有传输和 AWS。 Resource Groups 使用传输层安全 (TLS) 1.2，但也支持 TLS 1.0 和 1.1。

的身份和访问管理 AWS Resource Groups

AWS Identity and Access Management (IAM) 是一个 AWS 服务 可帮助管理员安全地控制对以下内容的访问权限 AWS 资源的费用。IAM管理员控制谁可以通过身份验证（登录）和授权（拥有权限）来使用 Resource Groups 资源。IAM是一个 AWS 服务 无需支付额外费用即可使用。

主题

受众

你怎么用 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您在资源组（Resource Groups）中所做的工作。

服务用户 – 如果使用 Resource Groups 服务来完成工作，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 Resource Groups 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 Resource Groups 中的功能，请参阅 对 AWS Resource Groups 身份和访问进行故障排除。

服务管理员 – 如果您在公司负责管理 Resource Groups 资源，您可能具有 Resource Groups 的完全访问权限。您有责任确定您的服务用户应访问哪些 Resource Groups 功能和资源。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使用 Resourc IAM e Groups，请参阅Resource Groups 是如何使用的 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 Resource Groups 的访问权限。要查看您可以在中使用的基于身份的 Resource Groups 策略示例IAM，请参阅。AWS Resource Groups 基于身份的策略示例

使用身份进行身份验证

身份验证是您登录的方式 AWS 使用您的身份凭证。您必须经过身份验证（登录到 AWS) 作为 AWS 账户根用户、以IAM用户身份或通过担任IAM角色来完成。

你可以登录 AWS 使用通过身份源提供的凭证作为联合身份。 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。当你访问时 AWS 通过使用联合，您就是在间接担任角色。

根据您的用户类型，您可以登录 AWS Management Console 或者 AWS 访问门户。有关登录的更多信息 AWS，请参阅如何登录您的 AWS 账户中的 AWS 登录 用户指南。

如果你访问 AWS 以编程方式， AWS 提供了一个软件开发套件 (SDK) 和一个命令行界面 (CLI)，用于使用您的凭证对您的请求进行加密签名。如果你不使用 AWS 工具，你必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅签名 AWS APIIAM用户指南中的请求。

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) 来提高帐户的安全性。要了解更多信息，请参阅中的多重身份验证 AWS IAM Identity Center《用户指南》和《使用多因素身份验证》(MFA) AWS（在 IAM 用户指南中）。

AWS 账户 根用户

当你创建 AWS 账户，您从一个登录身份开始，该身份可以完全访问所有人 AWS 服务 以及账户中的资源。这个身份叫做 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。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”。

IAM 用户和组

IAM用户是你内心的身份 AWS 账户 对个人或应用程序具有特定权限。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）。

IAM角色

IAM角色是你内在的身份 AWS 账户 具有特定权限的。它与IAM用户类似，但与特定人员无关。你可以暂时扮IAM演一个角色 AWS Management Console 通过切换角色。你可以通过调用来扮演角色 AWS CLI 或者 AWS API操作或使用自定义URL。有关使用角色的方法的更多信息，请参阅《IAM用户指南》中的使用IAM角色。

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，请参阅中的权限集 AWS IAM Identity Center 用户指南。
- 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，有些 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 — 一些 AWS 服务 使用其他功能 AWS 服务。 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，你被视为校长。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使用委托人的权限调用 AWS 服务，再加上请求的 AWS 服务 向下游服务发出请求。FAS只有当服务收到需要与其他服务进行交互的请求时，才会发出请求 AWS 服务 或需要完成的资源。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，请参阅创建角色以向某人委派权限 AWS 服务（在 IAM 用户指南中）。
- 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。 该服务可以代替您执行操作。服务相关角色显示在您的 AWS 账户 并归该服务所有。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实例上运行的应用程序的临时证书 AWS CLI 或者 AWS API请求。这比在EC2实例中存储访问密钥更可取。要分配 AWS 在EC2实例中扮演角色并使其可供其所有应用程序使用，则可以创建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

您可以控制访问权限 AWS 通过创建策略并将其附加到 AWS 身份或资源。策略是中的一个对象 AWS 当与身份或资源关联时，它定义了他们的权限。 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。大多数策略都存储在 AWS 作为JSON文件。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用于指定谁有权访问什么的策略。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中获取角色信息 AWS Management Console，AWS CLI，或者 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，您可以将其附加到您的多个用户、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。你不能用 AWS 基于资源的策略IAM中的托管策略。

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。

亚马逊 S3， AWS WAF，Amazon 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 是指定组织或组织单位 (OU) 的最大权限的JSON策略 AWS Organizations. AWS Organizations 是一项用于对多个进行分组和集中管理的服务 AWS 账户 你的企业拥有的。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。SCP限制了成员账户中实体的权限，包括每个 AWS 账户根用户。 有关 Organization SCPs s 和的更多信息，请参阅中的服务控制策略 AWS Organizations 用户指南。

- 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。要了解如何做 AWS 决定在涉及多种策略类型时是否允许请求，请参阅《IAM用户指南》中的策略评估逻辑。

Resource Groups 是如何使用的 IAM

在使用管理IAM对资源组的访问权限之前，您应该了解哪些IAM功能可用于资源组。要全面了解 Resource Groups 和其他 AWS 服务的使用方式IAM，请参阅《IAM用户指南》IAM中的 “与之配合使用的AWS 服务”。

主题

- Resource Groups 基于身份的策略
- 基于资源的策略
- 基于 Resource Groups 标签的授权
- Resource Grou IAM ps

Resource Groups 基于身份的策略

使用IAM基于身份的策略，您可以指定允许或拒绝的操作和资源，以及允许或拒绝操作的条件。Resource Groups 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。

Resource Groups 中的策略操作在操作前使用以下前缀：`resource-groups:`。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 `resource-explorer`。

例如，要授予某人使用资源组`CreateGroup`API操作创建资源组组的权限，您需要在他们的策略中包含该`resource-groups:CreateGroup`操作。策略语句必须包含 `Action` 或 `NotAction` 元素。Resource Groups 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 Resource Groups 和标签编辑器操作，请使用逗号将它们隔开，如下所示：

```
"Action": [
      "resource-groups:action1",
      "resource-groups:action2",
      "resource-explorer:action3"
```

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

```
"Action": "resource-groups:List*"
```

要查看 Resource Groups 操作列表，请参阅IAM用户指南 AWS Resource Groups中的操作、资源和条件键。

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。

`Resource`JSON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) 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": "*"
```

唯一的 Resource Groups 资源是组。该组资源的格式如下：ARN

```
arn:${Partition}:resource-groups:${Region}:${Account}:group/${GroupName}
```

有关格式的更多信息ARNs，请参阅 Amazon 资源名称 (ARNs) 和 AWS 服务命名空间。

例如，要在语句中指定my-test-group资源组，请使用以下命令ARN：

```
"Resource": "arn:aws:resource-groups:us-east-1:123456789012:group/my-test-group"
```

要指定属于特定账户的所有组，请使用通配符（*）：

```
"Resource": "arn:aws:resource-groups:us-east-1:123456789012:group/*"
```

无法对特定资源执行某些 Resource Groups 操作，例如，用于创建资源的操作。在这些情况下，您必须使用通配符 （*)。

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

某些 Resource Groups API 操作可能涉及多个资源。例如，DeleteGroup 删除群组，因此调用主体必须具有删除特定组或所有组的权限。要在单个语句中指定多个资源，请ARNs用逗号分隔。

```
"Resource": [
  "resource1",
  "resource2"
]
```

要查看 Resource Groups 资源类型及其资源类型列表ARNs，并了解您可以使用哪些操作来指定每种资源，请参阅IAM用户指南 AWS Resource Groups中的操作、资源和条件键。ARN

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密钥。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。

Resource Groups 定义了自己的一组条件键，还支持使用一些全局条件键。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。

要查看 Resource Groups 条件键列表，并了解您可以使用哪些操作和资源使用条件键，请参阅IAM用户指南 AWS Resource Groups中的操作、资源和条件键。

示例

要查看基于 Resource Groups 身份的策略示例，请参阅 AWS Resource Groups 基于身份的策略示例。

基于资源的策略

Resource Groups 不支持基于资源的策略。

基于 Resource Groups 标签的授权

您可以将标签附加到 Resource Groups 中的组，或者在请求中将标签传递给 Resource Groups。要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。在创建或更新组时，可以将标签应用于此组。有关在 Resource Groups 中为组添加标签的更多信息，请参阅本指南中的 在中创建基于查询的群组 AWS Resource Groups 和 更新中的群组 AWS Resource Groups。

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，请参阅查看基于标签的组。

Resource Grou IAM ps

IAM角色是您的 AWS 账户中具有特定权限的实体。Resource Groups 没有或不使用服务角色。

将临时凭证用于 Resource Groups

在 Resource Groups 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

服务相关角色允许 AWS 服务访问其他服务中的资源以代表您完成操作。

Resource Groups 没有服务相关角色，也没有使用服务相关角色。

服务角色

此功能允许服务代表您担任服务角色。

Resource Groups 没有或不使用服务角色。

AWS适用于 AWS Resource Groups 的托管策略

AWS 托管式策略是由 AWS 创建和管理的独立策略。AWS 托管式策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住，AWS 托管式策略可能不会为您的特定使用场景授予最低权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的客户管理型策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新在 AWS 托管式策略中定义的权限，则更新会影响该策略所附加到的所有主体身份（用户、组和角色）。当新的 AWS 服务启动或新的 API 操作可用于现有服务时，AWS 最有可能更新 AWS 托管式策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

Resource Groups 的 AWS 托管策略

- ResourceGroupsServiceRolePolicy

AWS 托管策略：ResourceGroupsServiceRolePolicy

您不能将 `ResourceGroupsServiceRolePolicy` 附加到自己的 IAM 实体。此附加到服务相关角色的策略允许 Resource Groups 代表您执行操作。有关更多信息，请参阅为 Resource Groups 使用服务相关角色。

此策略授予 Resource Groups 检索有关您资源组中的资源以及这些资源所属的任何 AWS CloudFormation 堆栈的信息所需的权限。这可让 Resource Groups 为组生命周期事件功能生成 CloudWatch 事件。

要查看此 AWS 托管策略的最新版本，请参阅 IAM 控制台中的 `ResourceGroupsServiceRolePolicy`。

AWS 托管策略：ResourceGroupsandTagEditorFullAccess

将策略附加到主体实体时，会向实体授予策略中定义的权限。 AWS 托管策略可让您更轻松地为用户、组和角色分配适当的权限，而不必自己编写策略。

此策略授予对 Resource Groups 和标签编辑器功能的完全访问所需的权限。

要查看此 AWS 托管策略的最新版本，请参阅 IAM 控制台中的 ResourceGroupsandTagEditorFullAccess。

有关此策略的更多信息，请参阅 AWS 托管策略参考指南中的 ResourceGroupsandTagEditorFullAccess。

AWS 托管策略：ResourceGroupsandTagEditorReadOnlyAccess

将策略附加到主体实体时，会向实体授予策略中定义的权限。 AWS 托管策略可让您更轻松地为用户、组和角色分配适当的权限，而不必自己编写策略。

此策略授予对 Resource Groups 和标签编辑器功能的只读访问所需的权限。

要查看此 AWS 托管策略的最新版本，请参阅 IAM 控制台中的 ResourceGroupsandTagEditorReadOnlyAccess。

有关此策略的更多信息，请参阅 AWS 托管策略参考指南中的 ResourceGroupsandTagEditorReadOnlyAccess。

Resource Groups 对 AWS 托管策略的更新

查看有关 Resource Groups 的 AWS 托管策略更新的详细信息（从该服务开始跟踪这些更改开始）。有关此页面更改的自动提示，请订阅 Resource Groups 文档历史记录页面上的 RSS 源。

更改	说明	日期
策略更新 – ResourceGroupsandTagEditorFullAccess	Resource Groups 更新策略以包含其他 AWS CloudFormation 权限。	2023 年 8 月 10 日
策略更新 – ResourceGroupsandTagEditorReadOnlyAccess	Resource Groups 更新策略以包含其他 AWS CloudFormation 权限。	2023 年 8 月 10 日

更改	说明	日期
新策略 – ResourceGroupsServiceRolePolicy	Resource Groups 添加一项新策略来支持其服务关联角色。	2022 年 11 月 17 日
Resource Groups 开始跟踪更改	Resource Groups 为其 AWS 托管策略开启跟踪更改。	2022 年 11 月 17 日

为 Resource Groups 使用服务相关角色

AWS Resource Groups 使用 AWS Identity and Access Management（IAM）服务相关角色。服务相关角色是一种独特类型的 IAM 角色，它与 Resource Groups 直接相关。服务相关角色由 Resource Groups 预定义，并包含该服务代表您调用其它 AWS 服务 服务所需的一切权限。

服务相关角色可让您更轻松地设置 Resource Groups，因为您不必手动添加必要的权限。Resource Groups 定义了其服务相关角色的权限，并为每个角色设置信任策略以确保仅有 Resource Groups 服务可担任其角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其他 IAM 实体的权限策略。

有关支持服务相关角色的其他服务的信息，请参阅与 IAM 配合使用的 AWS 服务，并查找 Service-linked roles（服务相关角色）列中显示为 Yes（是）的服务。请选择 Yes 与查看该服务的服务相关角色文档的链接。

Resource Groups 的服务相关角色权限

Resource Groups 使用以下服务相关角色来支持组生命周期事件。在创建角色后，选择角色名称上的链接，即可在 IAM 控制台中查看该角色。

- AWSServiceRoleForResourceGroups

Resource Groups 使用此角色中的权限来查询拥有您资源的 AWS 服务，以帮助解决组成员资格问题并使组保持最新状态。它允许 Resource Groups 向 Amazon EventBridge 服务发出服务相关事件。

AWSServiceRoleForResourceGroups服务相关角色仅信任以下服务来担任该角色：

- resourcegroups.amazonaws.com

通过以下 AWS 托管策略将权限附加到角色。选择策略名称上的链接，在 IAM 控制台中查看策略。

- AWS### AWS Resource Groups #####

为 Resource Groups 创建服务相关角色

> **Important**
>
> 如果您在其他需要此角色所支持功能的服务中完成某个操作，此服务相关角色可以出现在您的账户中。有关更多信息，请参阅我的 AWS 账户 中出现的新角色。

要创建服务相关角色，请开启组生命周期事件功能。

编辑 Resource Groups 的服务相关角色

Resource Groups 不允许您编辑 AWSServiceRoleForResourceGroups 服务相关角色。在创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。不过，您可以使用 IAM 编辑角色的说明。有关更多信息，请参阅 IAM 用户指南中的编辑服务相关角色。

删除 Resource Groups 的服务相关角色

只有在关闭组生命周期事件之后，您才可以删除服务相关角色。

> **Important**
>
> - AWS 阻止您移除服务相关角色，直到您首次关闭创建该角色的组生命周期事件功能。
> - 我们建议您不要删除服务相关角色，前提是您的 AWS 账户 中包含任何资源组。如果您删除此角色，Resource Groups 服务将无法与其他 AWS 服务 交互来管理您的组。

手动删除 服务相关角色

使用 IAM 控制台、AWS CLI 或 AWS API 删除 AWSServiceRoleForResourceGroups 服务相关角色。有关更多信息，请参阅 IAM 用户指南中的删除服务相关角色。

Console

删除 Resource Groups 服务相关角色

1. 打开 IAM 控制台的“角色”页面。

2. 找到名为 AWSServiceRoleForResourceGroups 的角色，然后选中它旁边的复选框。
3. 选择 Delete (删除)。
4. 在框中输入角色的名称，然后选择删除，以确认您打算删除该角色。

角色从 IAM 控制台中的角色列表中消失。

AWS CLI

删除 Resource Groups 服务相关角色

要删除角色，请输入以下命令，其参数如图所示。不要替换任何值。

```
$ aws iam delete-service-linked-role \
    --role-name AWSServiceRoleForResourceGroups
{
    "DeletionTaskId": "task/aws-service-role/resource-groups.amazonaws.com/
AWSServiceRoleForResourceGroups/34e58943-e9a5-4220-9856-fc565EXAMPLE"
}
```

该命令返回一个任务 ID。实际的角色删除是异步进行的。您可以通过将提供的任务标识符传递给以下 AWS CLI 命令来检查角色删除的状态。

```
$ aws iam get-service-linked-role-deletion-status \
    --deletion-task-id "task/aws-service-role/resource-groups.amazonaws.com/
AWSServiceRoleForResourceGroups/34e58943-e9a5-4220-9856-fc565EXAMPLE"
{
    "Status": "SUCCEEDED"
}
```

Resource Groups 服务相关角色支持的区域

Resource Groups 支持在该服务可用的所有 AWS 区域 中使用服务相关角色。有关更多信息，请参阅 AWS 区域和终端节点。

AWS Resource Groups 基于身份的策略示例

默认情况下，IAM 主体（例如角色和用户）没有创建或修改 Resource Groups 资源的权限。它们还无法使用 AWS Management Console、AWS CLI 或 AWS API 执行任务。IAM 管理员必须创建 IAM 策略，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，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 Resource Groups 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。我们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 托管式策略 或 工作职能的 AWS 托管式策略。
- 应用最低权限 – 在使用 IAM policy 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 policy 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 policy，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 policy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，以帮助您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 Acess Analyzer 策略验证。
- Require multi-factor authentication（MFA）[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。若要在调用 API 操作时需要 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 Resource Groups 控制台和 API

要访问 AWS Resource Groups 和标签编辑器控制台，您必须拥有一组最低的权限。这些权限必须允许您列出和查看有关您的 AWS 账户中的 Resource Groups 资源的详细信息。如果您创建的基于身份的策略比所需的最低权限更严格，则无法为具有该策略的主体（IAM 角色或用户）按预期运行该控制台和 API 命令。

要确保这些实体仍可使用 Resource Groups，可向实体附加以下策略（或包含以下策略中列出的权限的策略）。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": [
        "resource-groups:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-explorer:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

有关授权访问 Resource Groups 的更多信息，请参阅本指南中的 授予使用权限 AWS Resource Groups 和标签编辑器。

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": "*"
        }
    ]
}
```

查看基于标签的组

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 Resource Groups 资源的访问。该示例说明了如何创建策略以允许查看资源，在此示例中为资源组。但是，仅当组标签 `project` 具有与调用主体附加的标签相同的 `project` 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主体。如果具有标签键 `project` 和标签值 `alpha` 的主体尝试查看资源组，则还必须对该组标记 `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 AWS Resource Groups 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将 Resource Groups 和 IAM 一起使用时可能遇到的常见问题。

主题

- 我无权在 Resource Groups 中执行操作
- 我无权执行 iam：PassRole
- 我想允许 AWS 账户之外的人访问我的 Resource Groups

我无权在 Resource Groups 中执行操作

如果 AWS Management Console 告诉您您无权执行某项操作，则必须联系管理员寻求帮助。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组的详细信息，但不具有 `resource-groups:ListGroups` 权限时，会发生以下示例错误。

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

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 `resource-groups:ListGroups` 操作访问 `my-test-group` 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 Resource Groups。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的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 Resource Groups 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，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许 AWS 账户之外的人访问我的 Resource Groups

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以担任角色。对于支持基于资源的策略或访问控制列表（ACL）的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 Resource Groups 是否支持这些功能，请参阅 Resource Groups 是如何使用的 IAM。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过联合身份验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（联合身份验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问的区别，请参阅 IA M 用户指南中的跨账户资源访问。

Resource Groups 中的日志记录和监控

所有 AWS Resource Groups 操作均在 AWS CloudTrail 中记录。

使用 AWS Resource Groups 记录 AWS CloudTrail API 调用

AWS Resource Groups 和标签编辑器与 AWS CloudTrail 集成，该服务提供 Resource Groups 或标签编辑器中的用户、角色或 AWS 服务采取的操作记录。CloudTrail 将对 Resource Groups 的所有 API 调用均作为事件捕获，包括来自 Resource Groups 或标签编辑器控制台的调用和对 Resource Groups API 的代码调用。如果您创建跟踪记录，则可以使 CloudTrail 事件持续传送到 Amazon S3 存储桶（包括 Resource Groups 的事件）。如果您不配置跟踪，则仍可在 CloudTrail 控制台中的 Event history（事件历史记录）中查看最新事件。使用 CloudTrail 收集的信息，您可以确定向 Resource Groups 发出了什么请求、发出请求的 IP 地址、请求方、请求时间以及其他详细信息。

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

CloudTrail 中的资源组信息

在您创建 AWS 账户时，将在该账户上启用 CloudTrail。当 Resource Groups 或标签编辑器控制台中发生活动时，该活动将记录在 CloudTrail 事件中，并与其他 AWS 服务事件一同保存在事件历史记录中。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 CloudTrail 事件历史记录查看事件。

要持续记录 AWS 账户中的事件（包括 Resource Groups 的事件），请创建跟踪记录。通过跟踪，CloudTrail 可将日志文件传送至 Amazon S3 桶。默认情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有 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 Simple Storage Service（Amazon S3）存储桶。此外，您可以配置其他AWS服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取行动。有关更多信息，请参阅：

- 创建跟踪概览
- CloudTrail 支持的服务和集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 从多个区域接收 CloudTrail 日志文件和从多个账户接收 CloudTrail 日志文件

CloudTrail 记录所有 Resource Groups 操作，AWS Resource Groups API 参考中介绍了这些操作。CloudTrail 中的 Resource Groups 操作显示为以 API 端点 `resource-groups.amazonaws.com` 为来源的事件。例如，对 `CreateGroup`、`GetGroup` 和

UpdateGroupQuery 操作的调用会在 CloudTrail 日志文件中生成条目。控制台中的标签编辑器操作由 CloudTrail 记录，并显示为以内部 API 端点 resource-explorer 为来源的事件。

每个事件或日志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身份用户的临时安全凭证发出的。
- 请求是否由其它 AWS 服务发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

了解 Resource Groups 日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 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 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

下面的示例显示了一个 CloudTrail 日志条目，该条目说明了 CreateGroup 操作。


```
{"eventVersion":"1.05",
"userIdentity":{
    "type":"AssumedRole",
    "principalId":"ID number:AWSResourceGroupsUser",
    "arn":"arn:aws:sts::831000000000:assumed-role/Admin/AWSResourceGroupsUser",
    "accountId":"831000000000","accessKeyId":"ID number",
    "sessionContext":{
        "attributes":{
            "mfaAuthenticated":"false",
            "creationDate":"2018-06-05T22:03:47Z"
            },
        "sessionIssuer":{
            "type":"Role",
            "principalId":"ID number",
            "arn":"arn:aws:iam::831000000000:role/Admin",
            "accountId":"831000000000",
            "userName":"Admin"
            }
        }
    },
"eventTime":"2018-06-05T22:18:23Z",
```

```
"eventSource":"resource-groups.amazonaws.com",
"eventName":"CreateGroup",
"awsRegion":"us-west-2",
"sourceIPAddress":"100.25.190.51",
"userAgent":"console.amazonaws.com",
"requestParameters":{
    "Description": "EC2 instances that we are using for application staging.",
    "Name": "Staging",
    "ResourceQuery": {
      "Query": "string",
      "Type": "TAG_FILTERS_1_0"
      },
    "Tags": {
      "Key":"Phase",
      "Value":"Stage"
      }
    },
"responseElements":{
    "Group": {
      "Description":"EC2 instances that we are using for application staging.",
      "groupArn":"arn:aws:resource-groups:us-west-2:831000000000:group/Staging",
      "Name":"Staging"
     },
    "resourceQuery": {
      "Query":"string",
      "Type":"TAG_FILTERS_1_0"
     }
    },
"requestID":"de7z64z9-d394-12ug-8081-7zz0386fbcb6",
"eventID":"8z7z18dz-6z90-47bz-87cf-e8346428zzz3",
"eventType":"AwsApiCall",
"recipientAccountId":"831000000000"
}
```


Resource Group 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。

Resource Group 中的恢复能力

AWS Resource Groups 对内部服务资源执行自动备份。这些备份不可由用户配置。静态和传输中的备份均经过加密。Resource Groups 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。

即使用户资源组完全丢失也不会导致客户数据丢失，因为大多数客户数据都是跨 AWS 可用区（AZ）复制的。如果您意外删除组，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。

Resource Groups 中的基础设施安全性

没有其他方法来隔离 Resource Groups 提供的服务或网络流量。如果适用，请使用 AWS特定隔离。您可以使用中的资源组（Resource Groups）API和控制台VPC来帮助最大限度地提高隐私和基础架构安全性。

作为一项托管服务 AWS Resource Groups ，受 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的API调用通过网络访问 Resource Groups。客户端必须支持以下内容：

- 传输层安全 (TLS)。我们需要 TLS 1.2，建议使用 TLS 1.3。
- 具有完美前向保密性的密码套件 ()，例如（Ephemeral Diffie-HellmanPFS）或（Elliptic C DHE urve Ephemeral Diffie-Hellman）。ECDHE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IAM委托人关联的私有访问密钥对请求进行签名。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。

Resource Groups 不支持基于资源的策略。

Resource Groups 的安全最佳实践

以下最佳实践是一般指导原则，并不代表完整安全解决方案。这些最佳实践可能不适合您的环境或不满足您的环境要求，请将其视为有用的考虑因素而不是惯例。

- 使用最低权限授予组访问权限的原则。Resource Groups 支持资源级权限。仅在特定用户需要时才授予特定组的访问权限。避免在向所有用户或所有组分配权限的策略声明中使用星号。有关最低权限的更多信息，请参阅 IAM 用户指南中的授予最低权限。
- 避免在公共字段中包含私有信息。组的名称视为服务元数据。组名称未加密。请勿在组名称中输入敏感信息。组描述是私有信息。

  请勿在标签键或标签值中放入私有或敏感信息。

- 在适当时使用基于标记的授权。Resource Groups 支持基于标签的授权。您可以为组添加标签，然后更新附加到您的 IAM 主体（例如用户和角色）的策略，以根据应用于组的标签来设置其访问级别。有关如何使用基于标签的授权的更多信息，请参阅 IAM 用户指南中的使用资源标签控制对 AWS 资源的访问权限。

  许多 AWS 服务支持基于其资源的标签的授权。请注意，可能会为组中的成员资源配置基于标签的授权。如果对组资源的访问受到标签的限制，则未经授权的用户或组可能无法对这些资源执行操作或自动化。例如，如果某个组中的 Amazon EC2 实例的标签键为 `Confidentiality`，标签值为 `High`，并且您无权对已标记 `Confidentiality:High` 的资源运行命令，那么即使资源组中的其他资源成功执行操作，您在 EC2 实例上执行的操作或自动化也将失败。有关哪些服务支持对其资源进行基于标签的授权的更多信息，请参阅 IAM 用户指南中的与 IAM 配合使用的 AWS 服务。

  有关为 AWS 资源制定标记策略的更多信息，请参阅AWS 标记策略。

资源组的服务限额

下表描述了 AWS Resource Groups （Resource Groups）中的配额。要调整配额，您可以在 Service Quotas 控制台中申请增加配额。

名称	默认值	可调整	描述
每个账户的资源组数	每个受支持的区域：100 个	是	您可以在此账户中创建的资源组的最大数量。资源组是符合特定标准的 AWS 资源集合。

AWS Resource Groups 文档历史记录

变更	说明	日期
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 8 月 1 日
支持更多资源类型	资源组（Resource Groups）和标签编辑器现在支持更多资源类型。	2024 年 5 月 30 日
更新了 AWS 托管策略和 ResourceGroupsandTagEditorFullAccess ResourceGroupsandTagEditorReadOnlyAccess	Resource Groups 更新了两个 AWS 托管策略以添加其他 AWS CloudFormation 权限。	2023 年 8 月 10 日
Resource Groups 的服务限额	现在，您可以使用 Service Quotas 查看 Resource Groups 的配额限制。	2023 年 6 月 29 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
标签编辑器信息已移至其自己的指南	标签编辑器的文档已从本指南中删除，并移至新的《标签编辑器用户指南》。	2022 年 12 月 13 日
资源组现在可以包含 Amazon Keyspaces（Apache Cassandra 兼容）的资源	AWS Resource Groups 现在支持将 Amazon Keyspaces（适用于 Apache Cassandra）的资源包含在资源组中。	2022 年 10 月 20 日
资源类型的弃用	标签编辑器不再支持以下资源类型：`AWS::RoboMaker::Ro`	2022 年 5 月 17 日

	`bot` 、`AWS::RoboMaker::Fleet` 和 `AWS::RoboMaker::DeploymentJob` 。	
新的 AWS 托管策略-ResourceGroupsServiceRolePolicy	Resource Groups 在 AWS Identity and Access Management (IAM) 中添加了一个新的 AWS 托管策略，以支持服务的服务相关角色。	2022 年 1 月 12 日
组生命周期事件	资源组现在可以在 Amazon Events 中生成 CloudWatch 事件，以便在资源组发生变化时提醒您。	2022 年 1 月 12 日
现在，Amazon VPC Network Access Analyzer 可以使用资源组来监控流向您的 AWS 资源的有害网络流量。	您可以使用 AWS Resource Groups 来指定网络访问要求的来源和目的地。	2021 年 12 月 3 日
增加了对 AWS 弹性中心资源的支持	AWS Resource Groups 现在支持在资源组中包含 AWS 弹性中心的资源。	2021 年 11 月 18 日
增加对 Amazon Pinpoint 资源的支持	AWS Resource Groups 现在支持在资源组中包含用于 Amazon Pinpoint 的资源。	2021 年 11 月 11 日
增加了对由配置和管理的资源组的支持 AppRegistry	AWS Resource Groups 现在支持包含您使用创建的应用程序中资源的服务配置的资源组 AWS Service Catalog AppRegistry。有关更多信息，请参阅《AWS Resource Groups API参考资料》中的服务配置。	2021 年 9 月 15 日

增加了对 Amazon OpenSearch 服务资源的支持	AWS Resource Groups 现在支持将 Amazon OpenSearch 服务的资源包括在资源组中。	2021 年 8 月 11 日
增加了对 AWS Braket 资源的支持	AWS Resource Groups 现在支持将 AWS Braket 的资源包含在资源组中。	2021 年 6 月 30 日
增加了对 Amazon EMR 容器资源的支持	AWS Resource Groups 现在支持在资源组中包含用于 Amazon EMR 容器的资源。	2021 年 4 月 27 日
增加了对其他 AWS 服务资源的支持	AWS Resource Groups 现在支持在资源组中包含以下服务的资源：Amazon CodeGuru Reviewer、Amazon Elastic Inference、Amazon Forecast、Amazon Fraud Detector 和服务配额。	2021 年 2 月 25 日
增加安全性和合规性章节。	讨论 Resource Groups 如何保护您的信息并遵守监管标准。	2020 年 7 月 30 日

增加对为 AWS 服务配置的资源组的支持	现在，您可以创建与 AWS 服务关联的资源组，并配置该服务如何与组中的资源进行交互。在该功能的第一个版本中，您可以创建一个包含 Amazon EC2 容量预留的资源组，然后在该组中启动 Amazon EC2 实例。如果组的一个或多个预留中存在与您实例匹配的容量，则该实例将使用此预留。如果该实例与组中的任何可用预留都不匹配，则它将作为按需实例启动。有关更多信息，请参阅 Amazon EC2 用户指南中的使用容量预留组。	2020 年 7 月 29 日
增加了对 AWS IoT Greengrass 资源的支持。	AWS Resource Groups 和标签编辑器现在支持更多资源类型。	2020 年 3 月 25 日

查看的操作数据 AWS Resource Groups	在 AWS Systems Manager 控制台中，该 AWS Resource Groups 页面在四个选项卡上显示选定群组的操作数据：“详细信息”、“Config” CloudTrail、、OpsItems。在 Resource Groups 控制台中查看组时，这些选项卡不可用。您可以使用这些选项卡上的信息来帮助您了解组中的哪些资源符合要求并且正常工作，以及哪些资源需要操作。如果需要对资源执行操作，则可以使用 Systems Manager 自动化运行手册执行常见的操作维护和故障排除任务。有关更多信息，请参阅 AWS Systems Manager 用户指南 AWS Resource Groups中的查看 的操作数据。	2020 年 3 月 16 日
检查标签策略的合规性	使用创建标签策略并将其附加到账户后 AWS Organizations，您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
支持更多资源类型	AWS Resource Groups 和标签编辑器现在支持更多资源类型。	2019 年 10 月 4 日
支持的新资源类型 AWS Resource Groups	现在支持更多资源类型 AWS Resource Groups，特别是对于基于 AWS CloudFormation 堆栈的群组。	2019 年 8 月 5 日

支持的新资源类型 AWS Resource Groups	中现在支持的资源类型是 Amazon API Gatew REST APIs ay、Amazon Events CloudWatch 事件和亚马逊 SNS主题 AWS Resource Groups。	2019 年 6 月 27 日
标签编辑器现在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
AWS Resource Groups 和标签编辑器支持的新资源类型	新增了 50 多种资源类型 AWS Resource Groups 并支持标签编辑器。	2019 年 6 月 6 日
AWS Resource Groups 标签编辑器控制台移出 AWS Systems Manager 控制台	AWS Resource Groups 和标签编辑器控制台现在独立于 Systems Manager 控制台。尽管您仍然可以在 Systems Manager 的左侧导航栏中找到指向 AWS Resource Groups 控制台的指针，但您可以直接从左上角的下拉菜单中打开资源组和标签编辑器控制台。AWS Management Console	2019 年 6 月 5 日
新的 Resource Groups 授权和访问控制功能	Resource Groups 现在支持基于操作的策略、资源级权限和基于标签的授权。	2019 年 5 月 24 日
较旧的传统资源组和标签编辑器工具不再可用	已删除提及较旧的经典或传统资源组和标签编辑器的内容；这些工具在 AWS中不再可用。改用 AWS Resource Groups 和标签编辑器。	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
为新的标签编辑器添加了文档	“使用标签编辑器” 部分介绍了如何使用全新的 AWS 标签编辑器控制台体验。	2019 年 2 月 13 日

Resource Groups 中的组支持新的资源类型	增加在 Resource Groups 中现在支持的新资源类型。	2019 年 2 月 4 日
改善了将标签添加到基于标签的 Resource Groups 查询的用户体验	对在基于标签的查询中添加标签的控制台用户体验进行了较小的更改。	2018 年 12 月 17 日
AWS CloudFormation Resource Groups 中增加了基于堆栈的查询支持	您可以根据 AWS CloudFormation 堆栈创建查询所在的资源组。在选择一个堆栈后，您可以从该堆栈中选择要在组的查询中显示的资源类型。	2018 年 11 月 13 日
Resource Groups CloudTrail	Resource Groups 现在提供 AWS CloudTrail 支持。您可以在中查看和处理所有 Resource Groups API 调用的日志 CloudTrail。	2018 年 6 月 29 日

- API版本：2017-11 -27
- 最近文档更新时间：2019 年 9 月 24 日

早期更新

下表描述了 2018 年 6 月之前每次发布 AWS Resource Groups 用户指南 时进行的重要更改。

更改	描述	日期
初始版本	新一代的首次发布 AWS Resource Groups	2017 年 11 月 29 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。